Plan Maestro de Seguridad basado en ISO/IEC 27001:2013

Empresa: Ingeniería SL

Autor: Antonio Romero Leña

Centro: Universitat Oberta de Catalunya

Agradecimientos:

A mis padres: por traerme hasta aquí.
A Inés y a mis amigos: por su infinita paciencia durante el desarrollo del Máster.

Licencia CC BY-NC-ND 3.0 ES

INDICE

0. RESUMEN 6

1. SITUACIÓN ACTUAL: CONTEXTUALIZACIÓN, OBJETIVOS Y ANÁLISIS DIFERENCIAL 7

1.1 Introducción a la ISO/IEC 27001 e ISO/IEC 27002 7
1.2 Contextualización y alcance 7
1.2.1 DESCRIPCIÓN DE LA EMPRESA 7
1.2.2 ÁREAS DE NEGOCIO 8
1.2.3 RECURSOS HUMANOS Y ESTRUCTURA ORGANIZACIONAL 8
1.2.4 DISTRIBUCIÓN Y ACTIVOS FÍSICOS. 10
1.2.5 DIAGRAMA DE RED 11
1.2.6 ESTADO INICIAL DE LA SEGURIDAD 11
1.3 Alcance 12
1.4 Objetivos del Plan director de Seguridad 12
1.5 Análisis diferencial con respecto la ISO/IEC 27001+ISO/IEC27002 13
1.5.1 ANÁLISIS DIFERENCIAL CON RESPECTO LA ISO/IEC 27001:2013 14
1.5.2 ANÁLISIS DIFERENCIAL CON RESPECTO LA ISO/IEC 27002:2013 16
1.5.3 CONCLUSIONES 20

2. SISTEMA DE GESTIÓN DOCUMENTAL 21

2.1 Introducción 21
2.2 Esquema documental 21
2.2.1 POLÍTICA DE SEGURIDAD 21
2.2.2 PROCEDIMIENTO DE AUDITORÍAS INTERNAS 21
2.2.3 GESTIÓN DE INDICADORES 22
2.2.4 PROCEDIMIENTO DE REVISIÓN POR DIRECCIÓN 22
2.2.5 GESTIÓN DE ROLES Y RESPONSABILIDADES 23
2.2.6 METODOLOGÍA DE ANÁLISIS DE RIESGOS 23
2.2.7 DECLARACIÓN DE APLICABILIDAD 23

3. ANÁLISIS DE RIESGOS 24

3.1 Introducción 24
3.2 Inventario de activos 24
3.3 Valoración de los activos 26
3.4 Dimensiones de seguridad 28
3.5 Tabla resumen de valoración 28
3.6 Análisis de amenazas 30
3.7 Impacto potencial 39
3.8 Nivel de Riesgo Aceptable y Riesgo Residual 41
3.9 Resultados 43

4. PROPUESTAS DE PROYECTOS 46

4.1 Introducción 46
4.2 Propuestas de proyectos 46

4.3 Resultados 47
4.3.1 EVOLUCIÓN DEL RIESGO TRAS LA EJECUCIÓN DE LOS PROYECTOS 47
4.3.1 NIVEL DE CUMPLIMIENTO RESPECTO A LA NORMA 50

5. AUDITORÍA DE CUMPLIMIENTO 55

5.1 Introducción 55
5.2 Metodología 55
5.3 Alcance 56
5.4 Evaluación de la Madurez 56
5.5 Resultados 64

6. CONCLUSIONES 65

6.1 Situación inicial y objetivos del Plan: 65
6.2 Objetivos conseguidos 65
6.3 Objetivos futuros 66

7. GLOSARIO DE TÉRMINOS 67

8. BIBLIOGRAFÍA Y REFERENCIAS 68

9. ANEXOS 69

0. Resumen

El presente documento consiste en la elaboración de un Plan Director de Seguridad para la empresa Ingeniería S.L, como proyecto final del Máster Interuniversitario en Seguridad de la Información de las TIC (MISTIC). Este plan, seguirá el estándar de la ISO/IEC 27001:2013 para la implementación de un Sistema de Gestión de la Seguridad de la Información (SGSI).

El Plan Director de Seguridad deberá estar alineado con el negocio desarrollado por la empresa Ingeniería SL y servirá a la organización como punto de partida para la mejora de la gestión de la seguridad dentro de un modelo de mejora continua PDCA (PLAN-DO-CHECK-ACT).

El proyecto se iniciará con una descripción inicial, en la que se analizará el contexto de la organización, alcance del proyecto, objetivos del Plan y un análisis diferencial respecto a las normas ISO/IEC 27001:2013 y ISO/IEC 27002:2013. Posteriormente se definirá un Sistema de Gestión Documental para después pasar a la realización de un Análisis de riesgos mediante la metodología MAGERIT. Tomando este análisis como base, en la siguiente fase, se propondrán una serie de proyectos para buscar los objetivos definidos inicialmente. Una vez llegados a este punto, se realizará una Auditoría de Cumplimiento de la ISO/IEC 27002:2013 que evaluará los controles implementados y el cumplimiento de los objetivos definidos. Para finalizar, se realizará un informe de los resultados obtenidos y una presentación ejecutiva a la Dirección de la organización Ingeniería SL.

1. Situación actual: contextualización, objetivos y análisis diferencial

1.1 Introducción a la ISO/IEC 27001 e ISO/IEC 27002

Todas las organizaciones almacenan y procesan, de uno u otro modo, información. Esta información, en sus diferentes formas, es un activo muy valioso para el negocio de la organización y para los procesos internos de la propia organización, y, por tanto, requiere de un adecuado tratamiento que asegure su correcta gestión. Una gestión de la seguridad eficaz garantizará a la dirección y al resto de partes interesadas, como proveedores o clientes, que los activos de la organización están razonablemente protegidos.

Hay que indicar, que la seguridad de la información no se limita a la seguridad de los Sistemas de Información o de las Tecnologías de la Información, como pueden ser los elementos técnicos que la procesan, servidores, routers, etc., sino que también se aplica y engloba a la gestión de todos los procesos de la organización, como pueden ser los procesos del área comercial, los recursos humanos, la protección física de las instalaciones, etc.

Para la gestión eficaz de la seguridad de la información, han surgido varios estándares que sirven de guía para la implantación de un SGSI (Sistema de Gestión de la Seguridad de la Información). La norma ISO/IEC 27001 define la implementación de un SGSI y para ello, se utilizan los controles definidos en la norma ISO/IEC 27002.

Esta norma tiene su origen en la ISO/IEC 17799, que a su vez está basada en la norma británica BS 7799-1 publicada en 1995. Posteriormente, se publicó la ISO/IEC 17799:2005, que pasó a renombrarse como ISO/IEC 27002:2005. Más adelante, se publicó la última versión hasta el momento, la ISO/IEC 27002:2013.

Esta norma consiste en una guía para la implementación de los controles de seguridad y las prácticas más eficaces para gestionar la seguridad de la información en cualquier organización. Es importante indicar, que la norma no define un tamaño ni un tipo de organización, y, por tanto, es aplicable a cualquier tipo y tamaño de esta.

La ISO/IEC 27002 no es certificable, pero si lo es la 27001, que hace uso de los controles definidos en la 27001 para la implementación de un SGSI certificado.

1.2 Contextualización y alcance

1.2.1 Descripción de la empresa

La organización para la que se realizará el Plan Director será la empresa Ingeniería SL. Se trata de una empresa de base tecnológica (EBT) nacida en 2009 a partir de la iniciativa de tres profesores de Ingeniería Mecánica con una gran experiencia en Dinámica de sistemas Multicuerpo.

Ingeniería SL dispone de un equipo técnico que ha desarrollado su carrera profesional en el ámbito de la investigación universitaria en diferentes países, lo que otorga a la organización una fuerte orientación hacia proyectos de innovación, concretamente en tecnologías basadas en la mecánica computacional para la mejora de vehículos y equipos industriales.

En este momento, Ingeniería SL, se encuentra desarrollando tecnologías propias que le permitan crecer y convertirse en referente internacional en mecánica computacional. Para ello, mantiene fuertes relaciones con el ámbito de investigación universitario, tanto a nivel científico, mediante la colaboración en distintos proyectos, como a nivel humano, mediante la contratación de los ingenieros e investigadores más brillantes de la universidad con la que colabora. Además, también realiza proyectos internos de I+D mediante financiación púbica.

Como parte de su estrategia, Ingeniería SL invierte en su equipo humano buscando alcanzar un conocimiento difícilmente imitable por la competencia, lo que le otorga una ventaja competitiva, ya que este conocimiento se convierte en una barrera de entrada a competidores sobre sus líneas de negocio. Sin embargo, como se verá en el análisis de riesgos, estas ventajas pueden suponer un riesgo debido a la fuerte dependencia con sus recursos humanos que manejan este conocimiento.

Las empresas clientes de Ingeniería SL son organizaciones de referencia en sus mercados y basan su relación con Ingeniería SL en su estrategia en I+D+I, lo que implica que sus trabajos tienen una gran necesidad de gestionar correctamente la seguridad de la información, ya que manejan prototipos de procesos y productos altamente confidenciales para sus clientes.

1.2.2 Áreas de negocio

En general, Ingeniería SL desarrolla software a medida para simulaciones basadas en mecánica computacional. Asimismo, también desarrolla equipos electrónicos como soporte para los proyectos de simulación o de forma independiente para los mismos clientes.

Actualmente, existen principalmente, dos grandes áreas de negocio en Ingeniería SL: Termosolar y Ferrocarril. Como se ha indicado durante la descripción, también se realizan algunos proyectos internos de I+D mediante financiación púbica.

- Área Termosolar: proyectos de simulaciones fluido-termo-mecánicas y diseños de componentes de alta temperatura y presión.

- Área Ferrocarril: proyectos de simulación dinámica computacional. Entre otros, el equipo de Ingeniería SL participó en el desarrollo de SAMS2000, que actualmente utiliza la empresa de ferrocarriles de E.E.U.U para el análisis computacional de sus ferrocarriles.

- Proyectos I+D internos: se trata del desarrollo de herramientas propias que generan valor añadido a los proyectos externos y nuevas oportunidades de negocio.

1.2.3 Recursos humanos y Estructura organizacional

En este momento, la empresa Ingeniería SL, está formada por 3 socios que trabajan en la empresa y que cubren los puestos de director y directores de área, además de otros 3 empleados fijos y 2 eventuales.

Por otro lado, cuenta con los servicios externos de contabilidad, facturación y recursos legales. Y también dispone de un comercial externo que realiza las labores comerciales en el arranque de los proyectos, sobre todo en cuento a los contactos iniciales con clientes.

A continuación, se presenta gráficamente la estructura organizacional de Ingeniería SL, así como una breve descripción de los principales puestos y responsabilidades:

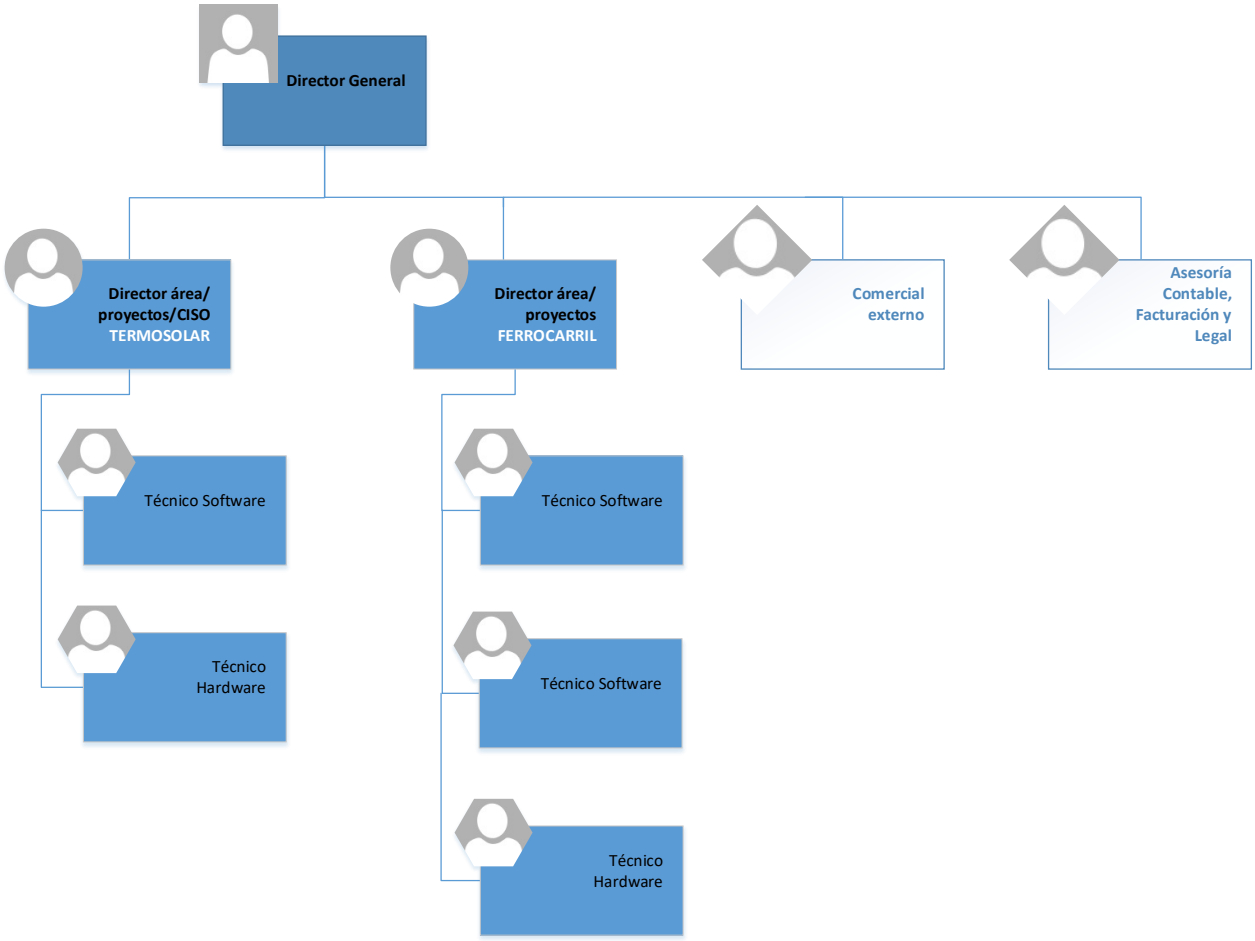


Ilustración 1

Director Gerente: CEO, CFO y relaciones con agentes externos.

Director de área Termosolar: jefe de proyectos del área. Planificación técnica y económica de los proyectos. CIO (Chief Information Officer). Soporte Pre-venta y Post-venta. También realiza funciones de CISO.

Director de área Ferrocarril: jefe de proyectos del área. Planificación técnica y económica de los proyectos. Soporte Pre-venta y Post-venta.

Ingeniero desarrollo software: uno de los ingenieros de desarrollo también realiza las funciones de CTO.

Como puede observarse en las descripciones anteriores, el CEO y los dos directores de área tienen otras responsabilidades además de estas, ya que, debido al tamaño de la empresa, no es posible disponer de recursos humanos específicos para todos los roles.

1.2.4 Distribución y activos físicos.

Las instalaciones de la empresa forman parte actualmente de una incubadora de empresas, donde realizan la mayor parte del trabajo. Este edificio les otorga los servicios de infraestructura básicos, como electricidad, agua, conexiones a internet y cableado estructurado. Actualmente, la empresa se encuentra iniciando el proceso de búsqueda de localizaciones para su traslado, debido sobre todo a su estrategia de crecimiento. Asimismo, también están llevando a cabo un proceso de expansión internacional, que por el momento incluye a Dinamarca, aunque todavía con una presencia física de forma intermitente mediante uno de los directores de área.

También se realiza parte del trabajo fuera de las instalaciones de la organización. Concretamente en las instalaciones de la universidad, en forma de subcontrataciones de laboratorios de ensayo para la realización de ensayos de nuevos desarrollos por parte de técnicos de Ingeniería SL.

La distribución física de las instalaciones de la organización es la siguiente:

Una oficina formada por 2 habitaciones comunicadas entre sí (A y B) a través de una puerta. Cada una de las habitaciones tiene salida directa al resto del edificio (pasillo compartido con otras empresas).

En la habitación A existe una sala de reuniones con puerta en una parte. En la otra, se dispone del servidor de datos y dos puestos de trabajo.

En la habitación B existe un espacio para reuniones abierto en una parte, y el resto de puestos de trabajo.

Los activos físicos de la organización son:

1 servidor de archivos, con GIT (software de control de versiones) y Redmine (software de gestión de proyectos).

Equipo electrónico: osciloscopio, generador de señal, placas para diseños electrónicos y herramientas varias.

3 Estaciones de trabajo.

4 PCs de escritorio.

3 portátiles.

1 pc de uso específico industrial.

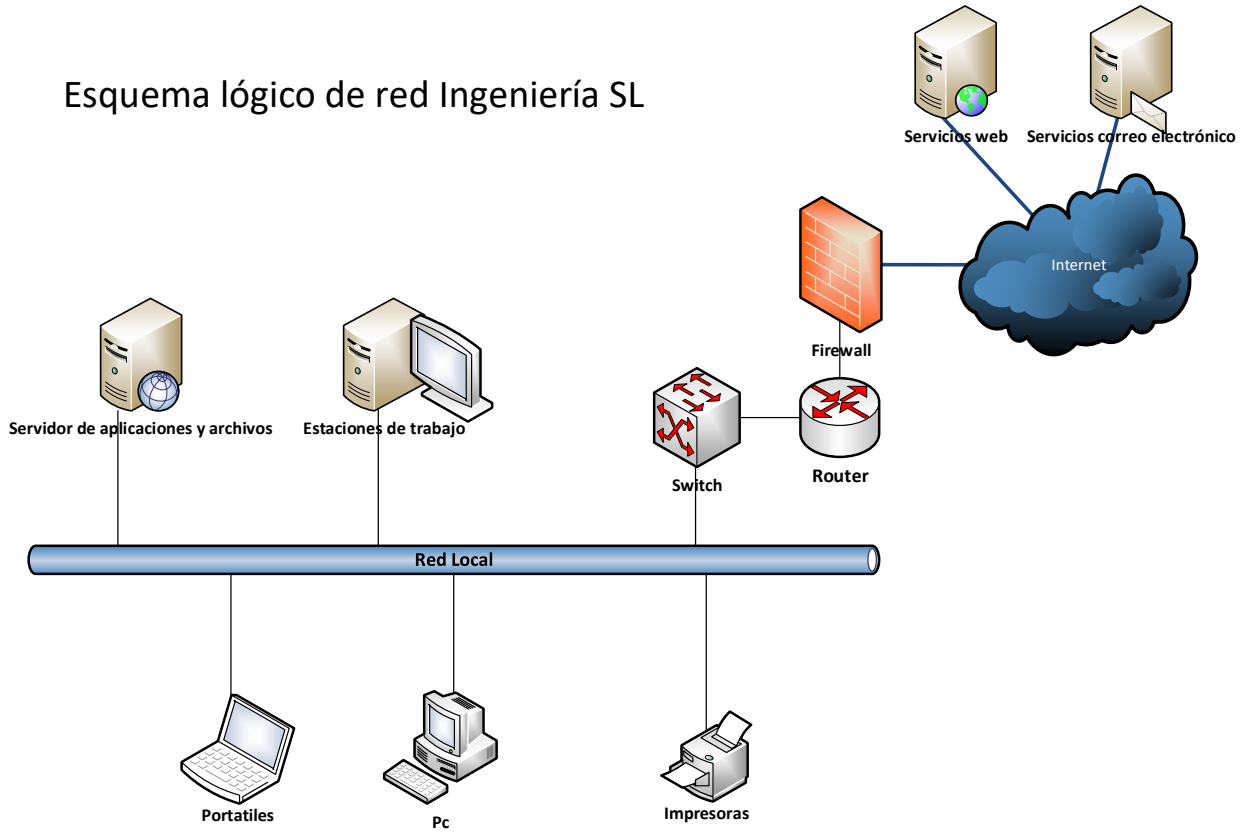
1 Router

2 switches

1 teléfono móvil.

Esta descripción, se ampliará cuando se realice el inventario de activos en fases posteriores del proyecto.

1.2.5 Diagrama de red



1.2.6 Estado inicial de la seguridad

La empresa no dispone de ningún estudio anterior sobre riesgos ni sobre la seguridad de la información.

A pesar de la falta de documentación y gestión de estos procesos, si tiene implantados algunos mecanismos de gestión de la seguridad de la información, aunque sin documentación en general, de forma que dependen completamente de la capacidad técnica y buenas prácticas de los usuarios. Estos mecanismos, son, por ejemplo, el plan de continuidad de negocio: si bien no existe un plan documentado, si se realizan copias de seguridad de toda la información relevante de forma periódica, con etiquetación adecuada y extracción de soportes a otras instalaciones seguras.

También se dispone parcialmente (solo sobre una parte de los datos) de etiquetado adecuado para la clasificación de la información. Además, parte de la gestión de la información en cuanto a inventariado y etiquetado se realiza mediante software específico de gestión de proyectos y de versiones.

Por otro lado, la dirección y el CIO tienen conciencia de esta falta de gestión de la seguridad de la información y de normativas y procedimientos que la mantengan. Anteriormente, se han producidos incidentes de seguridad que han afectado a la continuidad de la empresa, y, aunque pudieron ser subsanados con un coste de tiempos y recursos muy bajo, sirvió como toma de conciencia sobre la necesidad de una verdadera gestión de la información y de su seguridad.

1.3 Alcance

Es preciso definir un alcance del Plan director. Para ello, hay definir qué elementos de la organización serán analizados en este proyecto. Dado que todos los elementos que dispone esta organización, físicos, lógicos y humanos, son relevantes en cuanto a la gestión de la seguridad de la información, el alcance definido será el total de las instalaciones fijas de la organización, así como todos los equipos técnicos, recursos humanos y software de que dispone la empresa.

1.4 Objetivos del Plan director de Seguridad

Es muy importante definir unos objetivos concretos para los que se realizará este Plan Director. La organización no está interesada por el momento en la certificación de su Sistema de Gestión de la Seguridad de la Información, sobre todo porque tiene poco conocimiento real de su estado de la seguridad, aunque tiene mucho interés en conocerlo.

La Dirección y del CIO, han expresado su interés por conocer el estado de la seguridad de la información en su organización, así como por la imagen que representa este estado ante sus clientes actuales y potenciales, debido sobre todo a la información que manejan de estos. También reconocen que la falta de procesos normalizados y documentados para el tratamiento de la información no solo conlleva riesgos para la organización, si no que empeora la optimización de recursos y la gestión de las situaciones críticas, como pueden ser los incidentes de seguridad. Además, entiende que mediante un proceso de evaluación de riesgos y de creación de un Sistema de Gestión Documental, no solo harían frente de manera ordenada a los incidentes de seguridad, si no que mejoraría la optimización de recursos.

Por otro lado, la organización está actualmente buscando un nuevo emplazamiento, por lo que este trabajo también servirá para definir algunos requisitos necesarios para las nuevas instalaciones.

Para alinear este Plan Director con las necesidades de negocio, una vez entendidas estas, se proponen los siguientes objetivos para el Plan:

- Demostrar a clientes actuales y potenciales que se realiza una gestión adecuada para la protección de la información que manejan mediante el compromiso de la empresa con la seguridad de la información. Este Plan servirá de punto de partida para conocer el camino a seguir hacia la certificación de su SGSI, una vez esté implantado.
- Identificar los riesgos que pueden incidir en el negocio. Es importante señalar que la dirección no tiene claros que riesgos son asumibles y cuales tendrían unas consecuencias desastrosas en el negocio.
- Implantar las bases de un Sistema de Gestión Documental para la mejora de procesos y normalización de estos, para eliminar las situaciones actuales en las que la falta de documentación y el conocimiento no compartido, suponen un alto riesgo respecto a los recursos humanos empleados.
- Optimizar la respuesta a incidentes de seguridad.
- Valorar, con ayuda de este proyecto, los posibles nuevos emplazamientos que la empresa está buscando respecto a la distribución y seguridad física de las oficinas, dado que reconocen la necesidad de mejora en este sentido.

1.5 Análisis diferencial con respecto la ISO/IEC 27001+ISO/IEC27002

Para realizar un análisis diferencial respecto a las normas ISO/IEC 27001 y ISO/IEC 27001, se utilizará el Modelo de Madurez de la Capacidad (CMM) para valorar los controles de las normas. Mediante este modelo, se asignarán los valores según la siguiente tabla:

EFECTIVIDAD	CMM	SIGNIFICADO	DESCRIPCIÓN
0%	**L0**	Inexistente	Carencia completa de cualquier proceso reconocible. No se ha reconocido siquiera que existe un problema a resolver.
10%	**L1**	Inicial / Ad-hoc	Estado inicial donde el éxito de las actividades de los procesos se basa la mayoría de las veces en el esfuerzo personal. Los procedimientos son inexistentes o localizados en áreas concretas. No existen plantillas definidas a nivel corporativo.
50%	**L2**	Reproducible, pero intuitivo	Los procesos similares se llevan en forma similar por diferentes personas con la misma tarea. Se normalizan las buenas prácticas en base a la experiencia y al método. No hay comunicación o entrenamiento formal, las responsabilidades quedan a cargo de cada individuo. Se depende del grado de conocimiento de cada individuo.
90%	**L3**	Proceso definido	La organización entera participa en el proceso. Los procesos están implantados, documentados y comunicados mediante entrenamiento.
95%	**L4**	Gestionado y medible	Se puede seguir con indicadores numéricos y estadísticos la evolución de los procesos. Se dispone de tecnología para automatizar el flujo de trabajo, se tienen herramientas para mejorar la calidad y la eficiencia.
100%	**L5**	Optimizado	Los procesos están bajo constante mejora. En base a criterios cuantitativos se determinan las desviaciones más comunes y se optimizan los procesos.

Tabla 1

1.5.1 Análisis diferencial con respecto la ISO/IEC 27001:2013

Controles	Valoración
4.CONTEXTO DE LA ORGANIZACIÓN	
4.1 Comprensión de la organización y de su contexto	L1
4.2 Comprensión de las necesidades y expectativas de las partes interesadas	L1
4.3 Determinación del alcance del SGSI	L0
4.4 SGSI	L0
5. LIDERAZGO	
5.1 Liderazgo y compromiso	L1
5.2 Política	L0
5.3 Roles, responsabilidades y autoridades en la organización	L1
6. PLANIFICACIÓN	
6.1 Acciones para hacer frente a los riesgos y oportunidades	
6.1.1 General	L1
6.1.2 Valoración de los riesgos de seguridad de la información	L0
6.1.3 Tratamiento de los riesgos de seguridad de la información	L0
6.2 Objetivos de seguridad de la información y planificación para conseguirlos	L0
7. SOPORTE	
7.1 Recursos	L0
7.2 Competencia	L1
7.3 Concienciación	L1
7.4 Comunicación	L0
7.5 Información documentada	
7.5.1 General	L1
7.5.2 Creando y actualizando	L1
7.5.3 Control de la información documentada	L0
8. OPERACIÓN	
8.1 Planificación y control	L0
8.2 Valoración de los riesgos de la seguridad de la información	L0
8.3 Tratamiento de los riesgos de la seguridad de la información	L1
9. EVALUACIÓN DEL DESEMPEÑO	
9.1 Seguimiento, medición, análisis y evaluación	L0
9.2 Auditoría interna	L0
9.3 Revisión por la dirección	L0
10. MEJORA	
10.1 No conformidad y acciones correctivas	L0
10.2 Mejora continua	L0

Tabla 2

Una vez realizada la valoración de cada punto, podemos resumirla en la siguiente tabla de resultados:

Dominio	Conformidad (%)
4. Contexto de la organización	5
5. Liderazgo	6.7
6. Planificación	1,7
7. Soporte	5.3
8. Operación	3.3
9. Evaluación del desempeño	0
10. Mejora	0

Tabla 3

Por los valores de conformidad obtenidos, puede observarse claramente, que el nivel de conocimiento de la organización respecto al Sistema de Gestión de la Seguridad de la Información es prácticamente inexistente, lo que es lógico si llevamos la cuenta el estado inicial de la seguridad que se ha comentado de forma no cuantitativa anteriormente.

Con estos valores podemos visualizar, mediante una gráfica radial, el estado de ellos respecto al que sería óptimo:

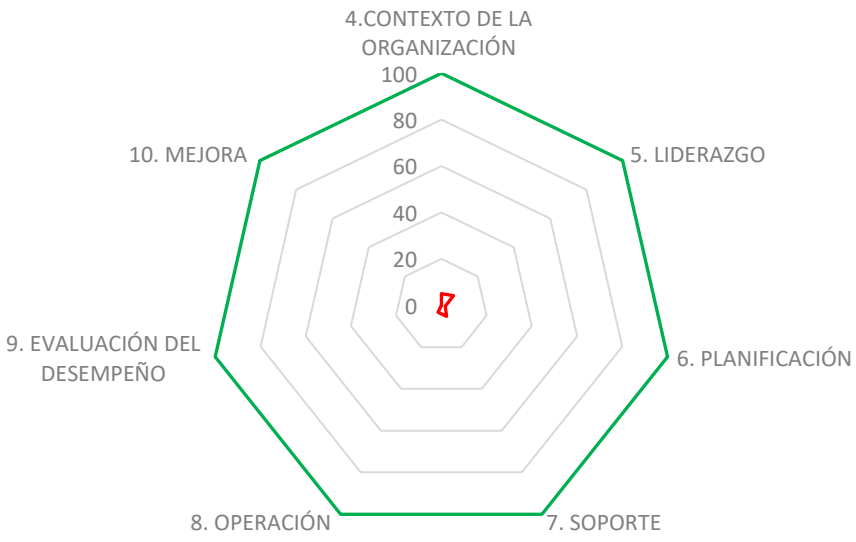


Ilustración 2

1.5.2 Análisis diferencial con respecto la ISO/IEC 27002:2013

A continuación, se valorarán, por cada dominio, todos los controles indicados en la ISO 27002, a partir del modelo DMM definido anteriormente:

Controles	Valoración
5. POLITICAS DE SEGURIDAD	
5.1 Directrices de la Dirección en seguridad de la información.	
5.1.1 Conjunto de políticas para la seguridad de la información.	L1
5.1.2 Revisión de las políticas para la seguridad de la información.	L1
6. ASPECTOS ORGANIZATIVOS DE LA SEGURIDAD DE LA INFORMACION	
6.1 Organización interna.	
6.1.1 Asignación de responsabilidades para la segur. de la información.	L2
6.1.2 Segregación de tareas.	L1
6.1.3 Contacto con las autoridades.	L2
6.1.4 Contacto con grupos de interés especial.	L1
6.1.5 Seguridad de la información en la gestión de proyectos.	L2
6.2 Dispositivos para movilidad y teletrabajo.	
6.2.1 Política de uso de dispositivos para movilidad.	L0
6.2.2 Teletrabajo.	L1
7. SEGURIDAD LIGADA A LOS RECURSOS HUMANOS	
7.1 Antes de la contratación.	
7.1.1 Investigación de antecedentes.	L0
7.1.2 Términos y condiciones de contratación.	L0
7.2 Durante el empleo.	
7.2.1 Responsabilidades de gestión.	L1
7.2.2 Concienciación, educación y capacitación en seguridad de la información.	L2
7.2.3 Proceso disciplinario.	L0
7.3 Finalización de empleo o cambio de puesto de trabajo.	
7.3.1 Responsabilidades ante la finalización o cambio	L0
8. GESTION DE ACTIVOS	
8.1 Responsabilidad sobre los activos.	
8.1.1 Inventario de activos.	L2
8.1.2 Propiedad de los activos.	L2
8.1.3 Uso aceptable de los activos.	L0
8.1.4 Devolución de activos.	L1
8.2 Clasificación de la información.	
8.2.1 Directrices de clasificación.	L2
8.2.2 Etiquetado y manipulado de la información.	L2
8.2.3 Manipulado de la información	L1
8.3 Manipulación de los soportes	
8.3.1 Gestión de soportes extraíbles.	L1
8.3.2 Eliminación de soportes.	L1
8.3.3 Soportes físicos en tránsito.	L0
9. CONTROL DE ACCESOS	
9.1 Requisitos de negocio para el control de accesos.	
9.1.1 Política de control de accesos.	L1
9.1.2 Acceso a las redes y a los servicios de red	L0

9.2 Gestión de acceso de usuario.	
9.2.1 Registro y baja de usuario.	L1
9.2.2 Provisión de acceso de usuario.	L2
9.2.3 Gestión de los derechos de acceso con privilegios especiales.	L1
9.2.4 Gestión de información secreta de autenticación de usuarios.	L1
9.2.5 Revisión de los derechos de acceso de usuario.	L0
9.2.6 Retirada o adaptación de los derechos de acceso	L2
9.3 Responsabilidades del usuario.	
9.3.1 Uso de información secreta para la autenticación.	L1
9.4 Control de acceso a sistemas y aplicaciones.	
9.4.1 Restricción del acceso a la información.	L2
9.4.2 Procedimientos seguros de inicio de sesión.	L1
9.4.3 Sistema de gestión de contraseñas.	L0
9.4.4 Uso de utilidades con privilegios de sistemas.	L1
9.4.5 Control de acceso al código fuente de los programas.	L2
10. CRIPTOGRAFIA	
10.1 Controles criptográficos.	
10.1.1 Política de uso de los controles criptográficos.	L0
10.1.2 Gestión de claves.	L0
11. SEGURIDAD FISICA Y AMBIENTAL	
11.1 Áreas seguras.	
11.1.1 Perímetro de seguridad física.	L1
11.1.2 Controles físicos de entrada.	L2
11.1.3 Seguridad de oficinas, despachos y recursos.	L1
11.1.4 Protección contra las amenazas externas y ambientales.	L1
11.1.5 El trabajo en áreas seguras.	L0
11.1.6 Áreas de acceso público, carga y descarga.	N/A
11.2 Seguridad de los equipos.	
11.2.1 Emplazamiento y protección de equipos.	L1
11.2.2 Instalaciones de suministro.	L1
11.2.3 Seguridad del cableado.	L2
11.2.4 Mantenimiento de los equipos.	L2
11.2.5 Retirada de materiales propiedad de la empresa	L1
11.2.6 Seguridad de los equipos y activos fuera de las instalaciones.	L0
11.2.7 Reutilización o retirada segura de dispositivos de equipos.	L1
11.2.8 Equipo de usuario desatendido.	L0
11.2.9 Política de puesto de trabajo despejado y bloqueo de pantalla.	L0
12. SEGURIDAD EN LAS OPERACIONES	
12.1 Procedimientos y responsabilidades operacionales.	
12.1.1 Documentación de procedimientos de operación.	L3
12.1.2 Gestión de cambios.	L2
12.1.3 Gestión de capacidades.	L1
12.1.4 Separación de los recursos de desarrollo, prueba y producción.	L2
12.2 Protección contra código malicioso.	
12.2.1 Controles contra el código malicioso.	L2
12.3 Copias de seguridad.	
12.3.1 Copias de seguridad de la información.	L2
12.4 Registros y supervisión.	
12.4.1 Registro de eventos	L2
12.4.2 Protección de la información de registro.	L2
12.4.3 Registros de administración y operación.	L1

12.4.4 Sincronización de relojes.	L1
12.5 Control del software en explotación.	
12.5.1 Instalación del software en sistemas en producción.	L2
12.6 Gestión de la vulnerabilidad técnica.	
12.6.1 Gestión de las vulnerabilidades técnicas.	L1
12.6.2 Restricciones en la instalación de software.	L0
12.7 Consideraciones de las auditorias de los sistemas de información.	
12.7.1 Controles de auditoria de los sistemas de información.	L0
13. SEGURIDAD EN LAS TELECOMUNICACIONES	
13.1 Gestión de la seguridad de redes.	
13.1.1 Controles de red.	L1
13.1.2 Seguridad de los servicios en red.	L0
13.1.3 Segregación en redes.	L0
13.2 Intercambio de información	
13.2.1 Políticas y procedimientos de intercambio de información.	L0
13.2.2 Acuerdos de intercambio de información.	L0
13.2.3 Mensajería electrónica.	L0
13.2.4 Acuerdos de confidencialidad o no revelación	L1
14. ADQUISICION, DESARROLLO Y MANTENIMIENTO DE LOS SISTEMAS DE INFORMACION	
14.1 Requisitos de seguridad en sistemas de información.	
14.1.1 Análisis de requisitos y especificaciones de seguridad de la información.	L0
14.1.2 Asegurar los servicios de aplicaciones en redes públicas.	L1
14.1.3 Protección de las transacciones de servicios de aplicaciones.	L1
14.2 Seguridad en los procesos de desarrollo y soporte.	
14.2.1 Política de desarrollo seguro de software.	L0
14.2.2 Procedimientos de control de cambios en los sistemas.	L1
14.2.3 Revisión técnica de las aplicaciones tras efectuar cambios en el sistema operativo	L0
14.2.4 Restricciones a los cambios en los paquetes de software.	L2
14.2.5 Uso de principios de ingeniería en protección de sistemas.	L1
14.2.6 Seguridad en entornos de desarrollo.	L2
14.2.7 Externalización del desarrollo de software.	L3
14.2.8 Pruebas de funcionalidad durante el desarrollo de los sistemas.	L1
14.2.9 Pruebas de aceptación.	L1
14.3 Datos de prueba.	
14.3.1 Protección de los datos utilizados en pruebas.	L1
15. RELACIONES CON SUMINISTRADORES	
15.1 Seguridad de la información en las relaciones con suministradores.	
15.1.1 Política de seguridad de la información para suministradores.	L0
15.1.2 Tratamiento del riesgo dentro de acuerdos de suministradores.	L0
15.1.3 Cadena de suministro en tecnologías de la información y comunicaciones	L0
15.2 Gestión de la prestación del servicio por suministradores.	
15.2.1 Supervisión y revisión de los servicios prestados por terceros.	L1
15.2.2 Gestión de cambios en los servicios prestados por terceros.	L1
16. GESTION DE INCIDENTES EN LA SEGURIDAD DE LA INFORMACION	
16.1 Gestión de incidentes de seguridad de la información y mejoras.	
16.1.1 Responsabilidades y procedimientos.	L1
16.1.2 Notificación de los eventos de seguridad de la información.	L1

16.1.3 Notificación de puntos débiles de la seguridad.	L0
16.1.4 Valoración de eventos de seguridad de la información y toma de decisiones	L0
16.1.5 Respuesta a los incidentes de seguridad.	L1
16.1.6 Aprendizaje de los incidentes de seguridad de la información.	L1
16.1.7 Recopilación de evidencias.	L0
17. ASPECTOS DE SEGURIDAD DE LA INFORMACION EN LA GESTION DE LA CONTINUIDAD DE NEGOCIO	
17.1 Continuidad de la seguridad de la información.	
17.1.1 Planificación de la continuidad de la seguridad de la información.	L1
17.1.2 Implantación de la continuidad de la seguridad de la información.	L0
17.1.3 Verificación, revisión y evaluación de la continuidad de la seguridad de la información	L0
17.2 Redundancias	
17.2.1 Disponibilidad de instalaciones para el procesamiento de la información	L0
18. CUMPLIMIENTO	
18.1 Cumplimiento de los requisitos legales y contractuales	
18.1.1 Identificación de la legislación aplicable.	L1
18.1.2 Derechos de propiedad intelectual (DPI).	L2
18.1.3 Protección de los registros de la organización.	L2
18.1.4 Protección de datos y privacidad de la información personal.	L2
18.1.5 Regulación de los controles criptográficos.	L1
18.2 Revisiones de la seguridad de la información.	
18.2.1 Revisión independiente de la seguridad de la información.	L0
18.2.2 Cumplimiento de las políticas y normas de seguridad.	L0
18.2.3 Comprobación del cumplimiento.	L0

Tabla 4

A partir de estas valoraciones, se pueden resumir por dominio, en la siguiente tabla:

Dominio	**Conformidad (%)**
5. Políticas de Seguridad	10
6. Aspectos Organizativos de la Seguridad de la Información	19,5
7. Seguridad ligada a los recursos humanos	6,7
8. Gestión de activos	23.6
9. Control de accesos	15,2
10. Criptografía	0
11. Seguridad Física y ambiental	15,8
12. Seguridad en las operaciones	33.6
13. Seguridad en las telecomunicaciones	2.9
14. Adquisición, desarrollo y mantenimiento de los sistemas de información	14
15. Relaciones con suministradores	5
16. Gestión de incidentes en la seguridad de la información	5,7
17. Aspectos de seguridad de la información en la gestión de la continuidad de negocio	1,6
18. Cumplimiento	1,7

Tabla 5

Como era de esperar, los valores de conformidad resultantes son bastante bajos. A continuación, se representan en forma de gráfica radial respecto al estado óptimo:

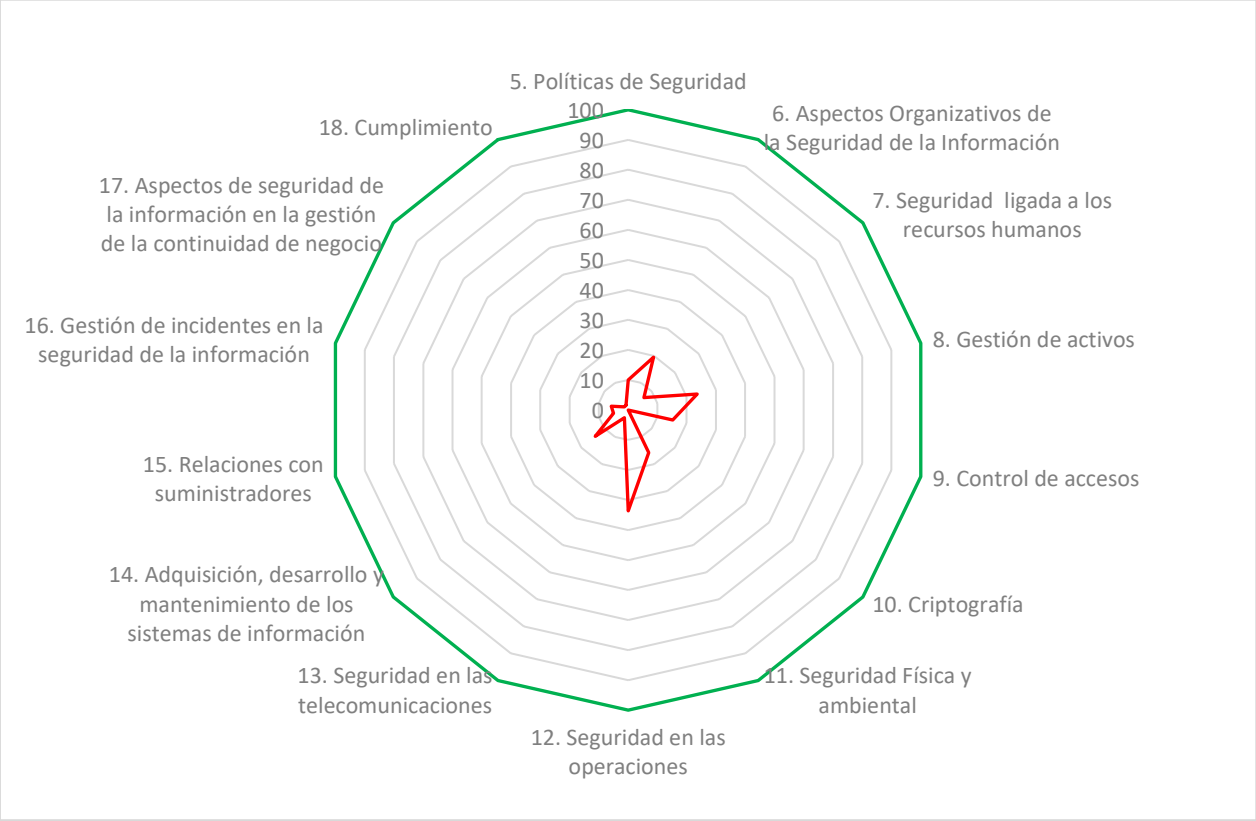


Ilustración 3

1.5.3 Conclusiones

A partir de los datos mostrados, podemos observar que la estimación inicial respecto al estado de la gestión de la seguridad era acertada. La organización no dispone de un sistema de gestión adecuado para el tratamiento de la seguridad de la información. Ni siquiera los valores más altos, dados en el dominio de la Seguridad en las operaciones o en la gestión de activos, se acercan a valores óptimos, por lo que queda claro que es necesaria la mejora en general en todos los dominios. Sin embargo, como se indicó inicialmente, no se busca en este momento la certificación de la norma, por lo que no se pretende la mejora en todos los dominios por igual, si no, en aquellos más relacionados con los objetivos definidos inicialmente. Esto no quiere decir que no se lleven en cuenta otros aspectos mejorables, pero no serán la prioridad cuando se realice la propuesta de proyectos, una vez que se tenga el análisis de riesgos.

A partir de la valoración efectuada y los objetivos que se definieron, la organización debería de concentrar los esfuerzos en generar documentación, tanto estructural como de los procesos más críticos. Asimismo, tendrá que definir las responsabilidades en la gestión de la información y definir políticas de buen uso de los materiales propios y en préstamo. En general, tendrá que trabajar sobre todo la documentación y normalización de los procesos que ya tiene definidos, aunque de una forma informal e intuitiva y definir y documentar algunos procesos críticos para los que no tiene ninguna referencia, como la gestión de la continuidad o de la gestión de incidentes.

2. Sistema de Gestión Documental

2.1 Introducción

Todos los Sistemas de Gestión requieren un sistema documental para el cumplimiento de la norma. De esta forma, el Sistema de Gestión de la Seguridad para la empresa Ingeniería SL requerirá un conjunto de documentos establecidos por la norma ISO/IEC 27001 y que serán el punto de partida para las siguientes fases del proyecto.

. Para este proyecto, se generarán los siguientes:

Política de seguridad

Procedimiento de Auditorías Internas

Gestión de Indicadores

Procedimiento de Revisión por Dirección

Gestión de Roles y Responsabilidades

Metodología de Análisis de Riesgos

Declaración de Aplicabilidad.

2.2 Esquema documental

2.2.1 Política de seguridad

La Política de Seguridad de la organización es un documento donde se establecen las directrices generales en seguridad de la información y que cuenta con el compromiso de la dirección de la organización. Además, debe estar alineada con los objetivos del negocio, así como con la legislación aplicable.

Para cumplir su objetivo, la Política de Seguridad debe ser comunicada claramente a todo el personal de la compañía y a colaboradores con acceso a información. Debe buscar además la implicación de todo el personal en cuanto a la seguridad de la información. En esta línea, el documento no deberá ser excesivamente técnico ni dar lugar a ambigüedades.

Esta política será revisada y aprobada anualmente por la Dirección.

El documento de la Política de seguridad se encuentra en el Anexo I.

2.2.2 Procedimiento de Auditorías internas

El Sistema de Gestión Documental de la organización debe de estar sujeto a un ciclo de mejora continua que incluye un proceso de auditorías internas para evaluar, de forma periódica, el estado del Sistema de Gestión de la Seguridad de la Información en cuanto a su implantación y consecución de los objetivos marcados.

Para la correcta realización de estas auditas, es preciso definir, entre otras cosas, el alcance y los mecanismos que se utilizarán para realizarlas. Asimismo, se definirá su planificación temporal para garantizar su periodicidad.

Este proceso queda definido en el Anexo II del presente documento.

2.2.3 Gestión de Indicadores

Será necesario definir los indicadores con los que poder medir el funcionamiento y la eficacia de los controles implantados. Para ello, se ha definido una tabla de indicadores con la descripción de cada uno, la frecuencia de medición, los valores objetivos a conseguir y los valores límites para la conformidad. Asimismo, cada indicador, tendrá un responsable de su medición.

A continuación, se describe cada parámetro con el que se definirán los indicadores:

Indicador: nombre del indicador definido.

Descripción: explicación del indicador

Frecuencia: periodicidad con la que se medirá el indicador

Valor objetivo: es el valor que se pretende conseguir, es decir, el valor óptimo que se debería medir con este indicador.

Valor umbral: es el valor límite máximo o mínimo (según sea mayor o menor que el valor objetivo), que permitirá establecer la conformidad del valor. Si el valor umbral es el mismo que el valor objetivo, significará que el indicador no tiene margen aceptable y solo permite el valor objetivo para darlo como conforme.

Responsable: se establece un responsable por cada indicador, de forma que será quien garantice que realicen las medidas adecuadas con la frecuencia establecida.

Para definir los indicadores, hay que llevar en cuenta la necesidad de cumplir el criterio SMART (Specific, Measurable, Assignable, Realistic), es decir, tiene que ser:

Específico: tiene que estar claramente definido y ser lo más concreto posible.

Medible: tiene que disponer de criterios de seguimiento y medición para verificar el cumplimiento.

Asignable: debe de poderse asignar a una persona o equipo de manera clara.

Realista: el indicador y su medida tienen que ser realistas.

La tabla con los indicadores se encuentra en el anexo III

2.2.4 Procedimiento de revisión por Dirección

Para que el Sistema de Gestión de la Seguridad de la Información funcione correctamente, deberá realizarse una revisión en la que la dirección de la organización deberá participar activamente. Estas revisiones deberán contar con los resultados de las auditorías internas y externas realizadas y deberán llevar en cuenta los posibles cambios en la empresa.

Este procedimiento deberá realizarse por la dirección junto con el comité de seguridad.

Este procedimiento se define en el Anexo IV

2.2.5 Gestión de Roles y Responsabilidades

Para la implantación del Sistema de Gestión de la Seguridad de la Información, ser requiere definir una estructura interna en la organización con las responsabilidades sobre la seguridad de la información. Esta estructura organizativa dependerá del tamaño y naturaliza de la organización y debe de ser aprobada por la dirección y contar con el apoyo de esta para dotarla de los recursos necesarios para ejercer sus funciones.

La definición de Roles y responsabilices queda definida en el Anexo V.

2.2.6 Metodología de Análisis de Riesgos

Se deberá establecer la metodología que se seguirá para calcular el riesgo en el posterior análisis de Riesgos, lo cual deberá incluir básicamente la identificación y valoración de los activos, amenazas y vulnerabilidades.

Esta metodología se describe en el Anexo VI.

2.2.7 Declaración de Aplicabilidad

Como indica la norma, deberá incluirse un documento con la selección de los controles de los dominios de ISO/IEC 27002:2013, que serán aplicables para el análisis de riesgos a efectuar. Este documento deberá ser aprobado por el comité de seguridad de Ingeniería SL.

Este documento se encuentra en el Anexo VII

3. Análisis de Riesgos

3.1 Introducción

En esta fase se realizará una evaluación de los activos de Ingeniería SL, mediante su identificación, las dependencias entre ellos y su valoración. También se analizarán las amenazas a las que están expuestos, su probabilidad de ocurrencia y el impacto sobre estos activos. Mediante este análisis, se podrá determinar el nivel de riesgo que la organización puede aceptar.

3.2 Inventario de activos

Para identificar los activos de Ingeniería SL, los organizaremos en los grupos, tal como se establece en la metodología MAGERIT. Para ello, utilizaremos los siguientes:

[L] Instalaciones

[HW] Equipamiento informático (hardware)

[SW] Software - Aplicaciones informáticas

[D] Datos / Información

[COM] Redes de comunicaciones

[S] Servicios

[AUX] Equipamiento auxiliar

[P] Personal

En la siguiente tabla se muestra el inventario completo de activos de Ingeniería SL:

Ámbito	Identificador	Activo	Cantidad
[L] Instalaciones			
	L.1	Sala Dirección	1
	L.2	Sala Producción	1
[HW] Equipamiento informático (hardware)			
	HW.1	Servidor	1
	HW.2	Estación de trabajo	3
	HW.3	PC de escritorio	4
	HW.4	PC Portátil	3
	HW.5	PC Industrial	1
	HW.6	Router (Fibra, Wifi, DHCP. FW)	1
	HW.7	Teléfono móvil	1
	HW.8	Teléfono fijo	2
	HW.9	Impresoras	2
	HW.10	Switch	2
	HW.11	Discos Backup	

[SW] Software - Aplicaciones informáticas			
	SW.1	Control de versiones GIT	
	SW.2	Gestión de proyectos REDMINE	
	SW.3	SUSE Linux Enterprise	
	SW.4	Ubuntu Linux	
	SW.5	Centos Linux	
	SW.6	MS Windows 10	3
	SW.7	MS Windows 7	4
	SW.8	Libre Office	
	SW.9	Thunderbird	
	SW.10	Antivirus Windows	5
[D] Datos / Información			
	D.1	Base de datos REDMINE	1
	D.2	Base de datos GIT	1
	D.3	Documentación compañía	
	D.4	Documentación interna	
	D.5	Datos clientes	
	D.6	Datos proveedores	
	D.7	Datos Proyectos	
[COM] Redes de comunicaciones			
	COM.1	Linea telefónica	1
	COM.2	Línea Internet	1
	COM.3	Línea móvil	1
	COM.4	Cableado oficina	
	COM.5	Red Wifi	1
[S] Servicios			
	S.1	Servicio de hosting, correo y dominio	1
	S.2	Electricidad	
[AUX] Equipamiento auxiliar			
	AUX.1	Equipamiento antiincencios	1
	AUX.2	Sistema de alarma	1
	AUX.3	Sistema de alimentación ininterrumpida	1
	AUX.4	Sistema climatización	1
	AUX.5	Armarios comunicaciones	2
[P] Personal			
	P.1	Director/gerente	1
	P.2	Director de Área	2
	P.3	Ingeniero desarrollo	3
	P.4	Ingeniero hardware i+d	2
	P.5	Comercial (externo)	1
	P.6	Contabilidad/Facturación (externo)	1

Tabla 6

3.3 Valoración de los activos

Para proteger los activos correctamente, primero es necesario establecer una valoración de estos. De esta manera, podrán establecerse las medidas necesarias para protegerlos sin incurrir en costes superiores a los de los propios activos a proteger.

Para realizar esta valoración, nos basaremos en la metodología MAGERIT. En ella se propone un análisis de los activos, clasificándolos en las categorías siguientes:

- MA: Muy alto
- A: Alto
- M: Medio
- B: Bajo
- M: Muy bajo

Además, se completará la clasificación con la estimación cuantitativa que se definió en el punto *2. Dimensionamiento y establecimiento de parámetros* del Anexo VI.

Para clasificar los activos correctamente, se llevará en cuenta la jerarquía existente entre ellos, para lo que se identificarán las dependencias entre ellos. Estas dependencias generan una estructura, que refleja como la seguridad de los activos superiores depende de la seguridad de sus activos inferiores. En la siguiente tabla se establece esta valoración:

Ámbito	Identificador	Activo	Valor	Dependencias
[L] Instalaciones				
	L.1	Sala Dirección	MA	
	L.2	Sala Producción	MA	
[HW] Equipamiento informático (hardware)				
	HW.1	Servidor	A	L.2 S.2 AUX.4 COM.4
	HW.2	Estación de trabajo	A	L.2 S.2 AUX.4
	HW.3	PC de escritorio	M	L.2 S.2
	HW.4	PC Portátil	M	L.2 L.1 S.2
	HW.5	PC Industrial	A	L.2 S.2
	HW.6	Router (Fibra, Wifi, DHCP. Firewall)	A	L.2 S.2
	HW.7	Teléfono móvil	MB	
	HW.8	Teléfono fijo	MB	L.1 L.2
	HW.9	Impresoras	B	L.2 S.2
	HW.10	Switch	M	L.1 L.2 S.2
	HW.11	Discos Backup	A	P.1
[SW] Software - Aplicaciones informáticas				
	SW.1	Control de versiones GIT	M	HW.1
	SW.2	Gestión de proyectos REDMINE	M	HW.1
	SW.3	SUSE Linux Enterprise	M	HW.2 HW.1

	SW.4	Ubuntu Linux	B	HW.3
	SW.5	Centos Linux	M	HW.3
	SW.6	MS Windows 10	B	HW.3
	SW.7	MS Windows 7	B	HW.4 HW.5
	SW.8	Libre Office	B	HW.3
	SW.9	Thunderbird	B	HW.3 COM.2 COM.4
	SW.10	Antivirus Windows	B	HW.3 HW4
[D] Datos / Información				
	D.1	Base de datos REDMINE	A	HW.1 SW.3
	D.2	Base de datos GIT	A	HW.1 SW.3
	D.3	Documentación compañía	A	HW.1 SW.3
	D.4	Documentación interna	M	HW.1 SW.3
	D.5	Datos clientes	M	HW.1 SW.3
	D. 6	Datos proveedores	M	HW.1 SW.3
	D.7	Datos Proyectos	MA	HW.1 SW.3
[COM] Redes de comunicaciones				
	COM.1	Línea telefónica	B	HW.8
	COM.2	Línea Internet	MA	HW.6
	COM.3	Línea móvil	MB	HW.7
	COM.4	Red de área local cableada	B	HW.10
	COM.5	Red Wifi	MB	HW.6
[S] Servicios				
	S.1	Servicio de hosting, correo y dominio	A	-
	S.2	Electricidad	MA	-
[AUX] Equipamiento auxiliar				
	AUX.1	Equipamiento antincendios	B	-
	AUX.2	Sistema de alarma	M	-
	AUX.3	Sistema de alimentación ininterrumpida	A	-
	AUX.4	Sistema climatización	A	S.2
	AUX.5	Armarios comunicaciones	B	
[P] Personal				
	P.1	Director/gerente	A	
	P.2	Director de Área	MA	
	P.3	Ingeniero desarrollo	A	
	P.4	Ingeniero hardware i+d	A	
	P.5	Comercial (externo)	M	
	P.6	Contabilidad/Facturación (externo)	M	

Tabla 7

3.4 Dimensiones de seguridad

Además de la valoración de cada activo, necesitamos conocer cuál es el aspecto de seguridad más crítico, para, de esta forma, orientar las posibles salvaguardas al aspecto que más interese para proteger el activo. Para conocer este dato, utilizaremos la valoración ACIDA de cada activo. Con esta valoración, se podrá después valorar el impacto que tendría la materialización de una amenaza sobre la parte del activo expuesto.

La valoración ACIDA permitirá trabajar con las distintas dimensiones de seguridad para cada activo, que serán:

- Autenticidad [A]
- Confidencialidad C]
- Integridad [I]
- Disponibilidad [D]
- Trazabilidad [A]

La valoración de cada dimensión se establecerá según los valores de la siguiente tabla:

Valor	Criterio
10	Daño muy grave para la organización
7-9	Daño grave para la organización
4-6	Daño importante a la organización
1-3	Daño menor a la organización
0	Irrelevante para la organización

Tabla 8

Respecto a las dependencias entre activos, los activos inferiores poseerán un valor acumulado del valor de los activos que se apoyan en ellos. Por ejemplo, el cableado de la red lan por sí mismo, solo dispondría de valoración en cuanto a su disponibilidad, no viéndose afectado por el resto de aspectos. Sin embargo, al apoyarse en él el activo Servidor, la valoración del cableado tendrá las valoraciones acumuladas del servidor, por lo que recibirá también su puntuación del resto de los aspectos críticos.

3.5 Tabla resumen de valoración

A partir de la valoración y las dimensiones de seguridad indicadas en los puntos anteriores, podemos realizar una tabla resumen de valoración:

Ámbito	Identificador	Activo	Valor	Aspectos Críticos				
				A	C	I	D	A
[L] Instalaciones								
	L.1	Sala Dirección	MA	8	10	10	10	8
	L.2	Sala Producción	MA	8	10	10	10	8
[HW] Equipamiento informático (hardware)								
	HW.1	Servidor	A	8	8	10	10	8

	HW.2	Estación de trabajo	A	8	8	10	10	5
	HW.3	PC de escritorio	M	3	8	5	8	5
	HW.4	PC Portátil	M	3	3	3	0	0
	HW.5	PC Industrial	A	3	3	5	5	3
	HW.6	Router (Fibra, Wifi, DHCP. Firewall)	A	8	8	8	10	3
	HW.7	Teléfono móvil	MB	3	3	0	0	0
	HW.8	Teléfono fijo	MB	0	0	0	0	0
	HW.9	Impresoras	B	0	0	0	3	0
	HW.10	Switch	M	3	3	3	10	3
	HW.11	Discos Backup	A	6	8	8	7	5
[SW] Software - Aplicaciones informáticas								
	SW.1	Control de versiones GIT	M	6	6	8	9	6
	SW.2	Gestión de proyectos REDMINE	M	6	6	8	9	6
	SW.3	SUSE Linux Enterprise	M	5	8	6	8	5
	SW.4	Ubuntu Linux	B	5	8	6	6	3
	SW.5	Centos Linux	M	3	3	5	5	3
	SW.6	MS Windows 10	B	5	7	6	7	3
	SW.7	MS Windows 7	B	5	5	6	7	3
	SW.8	Libre Office	B	5	3	5	5	3
	SW.9	Thunderbird	B	5	3	5	5	3
	SW.10	Antivirus Windows	B	6	7	7	8	6
[D] Datos / Información								
	D.1	Base de datos REDMINE	A	8	9	9	10	8
	D.2	Base de datos GIT	A	8	9	9	10	8
	D.3	Documentación compañía	A	5	6	5	8	7
	D.4	Documentación interna	M	5	7	7	6	7
	D.5	Datos clientes	M	9	8	6	3	5
	D. 6	Datos proveedores	M	5	7	6	3	6
	D.7	Datos Proyectos	MA	10	9	9	10	8
[COM] Redes de comunicaciones								
	COM.1	Línea telefónica	B	0	3	0	0	3
	COM.2	Línea Internet	MA	3	8	8	8	7
	COM.3	Línea móvil	MB	0	0	0	2	2
	COM.4	Red de área local cableada	B	8	8	10	10	8
	COM.5	Red Wifi	MB	0	0	0	2	0
[S] Servicios								
	S.1	Servicio de hosting, correo y	A	6	8	6	8	6

		dominio						
	S.2	Electricidad	MA	8	8	10	10	8
[AUX] Equipamiento auxiliar								
	AUX.1	Equipamiento antiincencios	B	0	0	0	9	0
	AUX.2	Sistema de alarma	M	0	0	0	8	0
	AUX.3	Sistema de alimentación ininterrumpida	A	0	0	0	9	0
	AUX.4	Sistema climatización	A	8	8	10	10	8
	AUX.5	Armarios comunicaciones	B	0	0	0	8	0
[P] Personal								
	P.1	Director/gerente	A	7	7	7	7	7
	P.2	Director de Área	MA	8	8	7	10	8
	P.3	Ingeniero desarrollo	A	8	8	7	9	8
	P.4	Ingeniero hardware i+d	A	8	8	6	9	8
	P.5	Comercial (externo)	M	8	5	2	6	3
	P.6	Contabilidad/Facturación (externo)	M	8	3	3	8	3

Tabla 9

3.6 Análisis de amenazas

Una vez valorados los activos de la organización, es necesario analizar las amenazas a las que están expuestos y como afectan estas a los diferentes aspectos de seguridad. Para ello, se analizarán como de vulnerable son los activos ante la materialización de una amenaza, llevando en cuenta una estimación de frecuencia de esta materialización.

Para llevar a cabo este estudio, se utilizará la clasificación de amenazas utilizadas en MAGERIT (capítulo 5, libro II. Catálogo de elementos), y que se presenta a continuación:

- [N] Desastres naturales: Sucesos que pueden ocurrir sin intervención de los seres humanos como causa directa o indirecta.

  [N.1] Fuego
  [N.2] Daños por agua
  [N.*] Desastres naturales

- [i] De origen industrial: Sucesos que pueden ocurrir de forma accidental, derivados de la actividad humana de tipo industrial. Estas amenazas puede darse de forma accidental o deliberada.

  [I.1] Fuego
  [I.2] Daños por agua
  [Ì.*] Desastres industriales

[I.3] Contaminación mecánica
[I.4] Contaminación electromagnética
[I.5] Avería de origen físico o lógico
[I.6] Corte de suministro eléctrico
[I.7] Condiciones inadecuadas de temperatura o humedad
[I.8] Fallo de servicios de comunicaciones
[I.9] Interrupción de otros servicios y suministros esenciales
[I.10] Degradación de los soportes de almacenamiento de información
[I.11] Emanaciones electromagnéticas

- [E] Errores y fallos no intencionados: Fallos no intencionales causados por las personas.

[E.1] Errores de los usuarios
[E.2] Errores del administrador
[E.3] Errores de monitorización (log)
[E.4] Errores de configuración
[E.7] Deficiencias en la organización
[E.8] Difusión de software dañino
[E.9] Errores de [re-]encaminamiento
[E.10] Errores de secuencia
[E.14] Escapes de información (Obsoleta. Sustituida por E.19)
[E.15] Alteración accidental de la información
[E.18] Destrucción de información
[E.19] Fugas de información
[E.20] Vulnerabilidades de los programas (software)
[E.21] Errores de mantenimiento / actualización de programas (software)
[E.23] Errores de mantenimiento / actualización de equipos (hardware)
[E.24] Caída del sistema por agotamiento de recursos
[E.25] Pérdida de equipos
[E.28] Indisponibilidad del personal

- [A] Ataques intencionados: Fallos deliberados causados por las personas.

[A.3] Manipulación de los registros de actividad (log)
[A.4] Manipulación de la configuración
[A.5] Suplantación de la identidad del usuario
[A.6] Abuso de privilegios de acceso
[A.7] Uso no previsto
[A.8] Difusión de software dañino
[A.9] [Re-]encaminamiento de mensajes
[A.10] Alteración de secuencia
[A.11] Acceso no autorizado
[A.12] Análisis de tráfico
[A.13] Repudio
[A.14] Interceptación de información (escucha)
[A.15] Modificación deliberada de la información
[A.18] Destrucción de información
[A.19] Divulgación de información
[A.22] Manipulación de programas
[A.23] Manipulación de los equipos
[A.24] Denegación de servicio
[A.25] Robo
[A.26] Ataque destructivo

[A.27] Ocupación enemiga
[A.28] Indisponibilidad del personal
[A.29] Extorsión
[A.30] Ingeniería social (picaresca)

MAGERIT establece, que cada amenaza no afecta a todos los tipos de activos ni tiene impacto en todas las dimensiones de seguridad. Por ejemplo, [A.29] Extorsión, solo aplica al activo Personal y solo impacto sobre las dimensiones de Confidencialidad, Integridad y Disponibilidad. En la tabla de frecuencias e impactos, solo aparecerán los que tengan aplicación.

Para la valoración de la frecuencia y el impacto de las amenazas sobre los activos, se tomarán los valores establecidos en el apartado 2. Dimensionamiento y establecimiento de parámetros del Anexo VI:

Frecuencia de la amenaza	Rango	Valor
Frecuencia Muy alta (MA)	1 vez al día	365/365 = 1
Frecuencia Alta (A)	1 vez cada 2 semanas	26/365 = 0.071233
Frecuencia Media (M)	1 vez cada 2 meses	6/365 = 0.016438
Frecuencia Baja (B)	1 vez cada seis meses	2/365 = 0.005479
Frecuencia Muy Baja (MB)	1 vez al año	1/365 = 0.002739

Tabla 10

Impacto	Valor
Muy alto (MA)	100%
Alto (A)	75%
Medio (M)	50%
Bajo (B)	20%
Muy Bajo (MB)	5%

Tabla 11

A continuación, se muestra la tabla con cada tipo de activo, la frecuencia de materialización de cada tipo de amenaza, la frecuencia resultante para cada tipo de activos (valor de frecuencia mayor de cada tipo de amenaza) y el impacto sobre las dimensiones de seguridad del activo.

Activos	**Amenazas**	**Frecuencia**	**Impacto**				
			A	C	I	D	A
[L] Instalaciones		MB (0.002739)					
L.1				100%	100%	100%	
L.2				100%	100%	100%	
	[N.1] Fuego	MB				100%	

	[N.2] Daños por agua	MB				100%	
	[N.*] Desastres naturales	MB				100%	
	[I.1] Fuego	MB				100%	
	[I.2] Daños por agua	MB				100%	
	[Ì.*] Desastres industriales	MB				100%	
	[I.11] Emanaciones electromagnéticas	MB		0%			
	[E.15] Alteración accidental de la información	MB			50%		
	[E.18] Destrucción de información	MB				75%	
	[E.19] Fugas de información	MB		50%			
	[A.7] Uso no previsto	MB		0%	0%	25%	
	[A.11] Acceso no autorizado	MB		100%	100%		
	[A.15] Modificación deliberada de la información	MB			100%		
	[A.18] Destrucción de información	MB				100%	
	[A.19] Divulgación de información	MB		100%			
	[A.26] Ataque destructivo	MB				100%	
	[A.27] Ocupación enemiga	MB		100%		100%	
[HW] Equipamiento informático (hardware)		M (0.016438)					
HW.1				100%	100%	100%	
HW.2				100%	100%	100%	
HW.3				100%	100%	100%	
HW.4				100%	100%	100%	
HW.5				100%	100%	100%	
HW.6				100%	100%	100%	
HW.7				100%	100%	100%	
HW.8				100%	100%	100%	
HW.9				100%	100%	100%	
HW.10				100%	100%	100%	
HW.11				100%	100%	100%	
	[N.1] Fuego	MB				100%	
	[N.2] Daños por agua	MB				100%	
	[N.*] Desastres naturales	MB				100%	
	[I.1] Fuego	MB				100%	
	[I.2] Daños por agua	MB				100%	
	[Ì.*] Desastres industriales	MB				100%	
	[I.3] Contaminación mecánica	MB				100%	
	[I.4] Contaminación electromagnética	MB				100%	
	[I.5] Avería de origen físico o lógico	B				100%	
	[I.6] Corte del suministro eléctrico	M				100%	
	[I.7] Condiciones	B				75%	

	inadecuadas de temperatura o humedad						
	[I.11] Emanaciones electromagnéticas	MB		0%			
	[E.2] Errores del administrador	MB		75%	100%	100%	
	[E.23] Errores de mantenimiento / actualización de equipos (hardware)	B				75%	
	[E.24] Caída del sistema por agotamiento de recursos	M				75%	
	[A.6] Abuso de privilegios de acceso	MB		50%	25%	25%	
	[A.7] Uso no previsto	MB		0%	0%	50%	
	[A.11] Acceso no autorizado	B		100%	100%		
	[A.23] Manipulación de los equipos	MB		50%		50%	
	[A.24] Denegación de servicio	M				100%	
	[A.25] Robo	MB		75%		100%	
	[A.26] Ataque destructivo	MB				100%	
[SW] Software - Aplicaciones informáticas		M (0.016438)					
SW.1			75%	100%	100%	100%	
SW.2			75%	100%	100%	100%	
SW.3			75%	100%	100%	100%	
SW.4			75%	100%	100%	100%	
SW.5			75%	100%	100%	100%	
SW.6			75%	100%	100%	100%	
SW.7			75%	100%	100%	100%	
SW.8			75%	100%	100%	100%	
SW.9			75%	100%	100%	100%	
SW.10			75%	100%	100%	100%	
	[I.5] Avería de origen físico o lógico	B				100%	
	[E.1] Errores de los usuarios	B		100 %	50%	100%	
	[E.2] Errores del administrador	MB		100%	100%	100%	
	[E.8] Difusión de software dañino	B		100%	100%	100%	
	[E.9] Errores de [re-] encaminamiento	MB		50%			
	[E.10] Errores de secuencia	MB			25%		
	[E.15] Alteración accidental de la información	MB			50%		
	[E.18] Destrucción de información	MB				75%	
	[E.19] Fugas de información	MB		25%			
	[E.20] Vulnerabilidades de	B		50%	75%	100%	

	los programas (software)						
	[E.21] Errores de mantenimiento / actualización de programas (software)	M			75%	100%	
	[A.5] Suplantación de la identidad del usuario	MB	75%	100%	100%		
	[A.6] Abuso de privilegios de acceso	MB		75%	75%	75%	
	[A.7] Uso no previsto	MB		0%	0%	75%	
	[A.8] Difusión de software dañino			100%	100%	100%	
	[A.9] [Re-]encaminamiento de mensajes	MB		100%			
	[A.10] Alteración de secuencia	MB			75%		
	[A.11] Acceso no autorizado	B		100%	100%		
	[A.15] Modificación deliberada de la información	MB			100%		
	[E.18] Destrucción de información	MB				100%	
	[A.19] Divulgación de información	MB		25%			
	[A.22] Manipulación de programas	MB		25%	100%	100%	
[D] Datos / Información		M (0.016438)					
D.1			75%	100%	100%	100%	100%
D.2			75%	100%	100%	100%	100%
D.3			75%	100%	100%	100%	100%
D.4			75%	100%	100%	100%	100%
D.5			75%	100%	100%	100%	100%
D.6			75%	100%	100%	100%	100%
D.7			75%	100%	100%	100%	100%
	[E.1] Errores de los usuarios	B		50%	50%	100%	
	[E.2] Errores del administrador	B		100%	100%	100%	
	[E.3] Errores de monitorización (log)	M					50%
	[E.4] Errores de configuración	B					100%
	[E.15] Alteración accidental de la información	MB			75%		
	[E.18] Destrucción de información	MB				100%	
	[E.19] Fugas de información	MB		100%			
	[A.3] Manipulación de los registros de actividad (log)	MB					50%
	[A.4] Manipulación de la configuración	MB		50%	50%	100%	
	[A.5] Suplantación de la	MB	75%	100%	100%		

	identidad del usuario						
	[A.6] Abuso de privilegios de acceso	MB		75%	75%	75%	
	[A.11] Acceso no autorizado	B		100%	100%		
	[A.13] Repudio	MB					50%
	[A.15] Modificación deliberada de la información	MB			100%		
	[E.18] Destrucción de información	MB				100%	
	[A.19] Divulgación de información	MB		100%			
[COM] Redes de comunicaciones		B (0.005479)					
COM.1			50%	100%	75%	100%	
COM.2			50%	100%	75%	100%	
COM.3			50%	100%	75%	100%	
COM.4			50%	100%	75%	100%	
COM.5			50%	100%	75%	100%	
	[I.8] Fallo de servicios de comunicaciones	B				100%	
	[E.2] Errores del administrador	MB		100%	50%	100%	
	[E.9] Errores de [re-] encaminamiento	MB		50%			
	[E.10] Errores de secuencia	MB			25%		
	[E.15] Alteración accidental de la información	MB			50%		
	[E.18] Destrucción de información	MB				50%	
	[E.19] Fugas de información	MB		25%			
	[E.24] Caída del sistema por agotamiento de recursos	MB				100%	
	[A.5] Suplantación de la identidad del usuario	MB	50%	75%	75%		
	[A.6] Abuso de privilegios de acceso	MB		50%	75%	75%	
	[A.7] Uso no previsto	MB		25%	0%	75%	
	[A.9] [Re-]encaminamiento de mensajes	MB		100%			
	[A.10] Alteración de secuencia	MB			75%		
	[A.11] Acceso no autorizado	B		100%	75%		
	[A.12] Análisis de tráfico	MB		75%			
	[A.14] Interceptación de información (escucha)	MB		100%			
	[A.15] Modificación deliberada de la información	MB			75%		
	[A.19] Divulgación de información	MB		25%			
	[A.24] Denegación de	MB				100%	

	servicio						
[S] Servicios		MB (0.002739)					
S.1			100%	100%	100%	100%	25%
S.2			100%	100%	100%	100%	25%
	[E.1] Errores de los usuarios	MB		100%	100%	100%	
	[E.2] Errores del administrador	MB		100%	100%	100%	
	[E.9] Errores de [re-] encaminamiento	MB		100%			
	[E.10] Errores de secuencia				25%		
	[E.15] Alteración accidental de la información	MB			50%		
	[E.18] Destrucción de información	MB				50%	
	[E.19] Fugas de información	MB		75%			
	[E.24] Caída del sistema por agotamiento de recursos	MB				50%	
	[A.5] Suplantación de la identidad del usuario	MB	100%	100%	50%		
	[A.6] Abuso de privilegios de acceso	MB		100%	75%	75%	
	[A.7] Uso no previsto	MB		50%	25%	100%	
	[A.9] [Re-]encaminamiento de mensajes	MB		100%			
	[A.10] Alteración de secuencia	MB			75%		
	[A.11] Acceso no autorizado	MB		100%	100%		
	[A.13] Repudio	MB					25%
	[A.15] Modificación deliberada de la información	MB			100%		
	[E.18] Destrucción de información	MB				75%	
	[A.19] Divulgación de información	MB		75%			
	[A.24] Denegación de servicio	MB				100%	
[AUX] Equipamiento auxiliar		M (0.016438)					
AUX.1				25%	100%	100%	
AUX.2				25%	100%	100%	
AUX.3				25%	100%	100%	
AUX.4				25%	100%	100%	
AUX.5				25%	100%	100%	
	[N.1] Fuego	MB				100%	
	[N.2] Daños por agua	MB				100%	
	[N.*] Desastres naturales	MB				100%	
	[I.1] Fuego	MB				100%	

	[I.2] Daños por agua	MB				100%	
	[Ì.*] Desastres industriales	MB				100%	
	[I.3] Contaminación mecánica	MB				100%	
	[I.4] Contaminación electromagnética	MB				100%	
	[I.5] Avería de origen físico o lógico	B				100%	
	[I.6] Corte del suministro eléctrico	M				100%	
	[I.7] Condiciones inadecuadas de temperatura o humedad	B				25%	
	[I.9] Interrupción de otros servicios y suministros esenciales	MB				25%	
	[I.11] Emanaciones electromagnéticas	MB		0%			
	[E.23] Errores de mantenimiento / actualización de equipos (hardware)	B				75%	
	[E.25] Pérdida de equipos	MB		0%		50%	
	[A.7] Uso no previsto	MB		0%	25%	75%	
	[A.11] Acceso no autorizado	MB		25%	100%		
	[A.23] Manipulación de los equipos	MB		0%		50%	
	[A.25] Robo	MB		0%%		100%	
	[A.26] Ataque destructivo	MB				100%	
[P] Personal		M (0.016438)		100%	75%	100%	
P.1				100%	75%	100%	
P.2				100%	75%	100%	
P.3				100%	75%	100%	
P.4				100%	75%	100%	
P.5				100%	75%	100%	
P.6				100%	75%	100%	
	[E.19] Fugas de información	MB		25%			
	[E.28] Indisponibilidad del personal	M				100%	
	[A.29] Extorsión	MB		100%	75%	100%	
	[A.30] Ingeniería social (picaresca)	MB		75%	75%	100%	

Tabla 12

3.7 Impacto potencial

El impacto potencial es el impacto que puede suponer para la organización la materialización de las amenazas. Dato que tenemos la valoración de los diferentes activos, podemos calcular el impacto potencial de la siguiente manera:

Impacto Potencial = Valor Activo x Porcentaje de Impacto

A continuación, se muestra una tabla con el cálculo del Impacto Potencial para cada activo:

Ámbito	ID	Valoración					Porcentaje de impacto (%)					Impacto Potencial				
		A	C	I	D	A	A	C	I	D	A	A	C	I	D	A
[L]																
	L.1	8	10	10	10	8		100	100	100		0	10	10	10	0
	L.2	8	10	10	10	8		100	100	100		0	10	10	10	0
[HW]																
	HW.1	8	8	10	10	8		100	100	100		0	8	10	10	0
	HW.2	8	8	10	10	5		100	100	100		0	8	10	10	0
	HW.3	3	8	5	8	5		100	100	100		0	8	5	8	0
	HW.4	3	3	3	0	0		100	100	100		0	3	3	0	0
	HW.5	3	3	5	5	3		100	100	100		0	3	5	5	0
	HW.6	8	8	8	10	3		100	100	100		0	8	8	10	0
	HW.7	3	3	0	0	0		100	100	100		0	3	0	0	0
	HW.8	0	0	0	0	0		100	100	100		0	0	0	0	0
	HW.9	0	0	0	3	0		100	100	100		0	0	0	3	0
	HW.10	3	3	3	10	3		100	100	100		0	3	3	10	0
	HW.11	6	8	8	7	5		100	100	100		0	8	8	7	0
[SW]																
	SW.1	6	6	8	9	6	75	100	100	100		4,5	6	8	9	0
	SW.2	6	6	8	9	6	75	100	100	100		4,5	6	8	9	0
	SW.3	5	8	6	8	5	75	100	100	100		3,75	8	6	8	0
	SW.4	5	8	6	6	3	75	100	100	100		3,75	8	6	6	0
	SW.5	3	3	5	5	3	75	100	100	100		2,25	3	5	5	0
	SW.6	5	7	6	7	3	75	100	100	100		3,75	7	6	7	0
	SW.7	5	5	6	7	3	75	100	100	100		3,75	5	6	7	0
	SW.8	5	3	5	5	3	75	100	100	100		3,75	3	5	5	0
	SW.9	5	3	5	5	3	75	100	100	100		3,75	3	5	5	0
	SW.10	6	7	7	8	6	75	100	100	100		4,5	7	7	8	0

[D]																
	D.1	8	9	9	10	8	75	100	100	100	100	6	9	9	10	8
	D.2	8	9	9	10	8	75	100	100	100	100	6	9	9	10	8
	D.3	5	6	5	8	7	75	100	100	100	100	3,75	6	5	8	7
	D.4	5	7	7	6	7	75	100	100	100	100	3,75	7	7	6	7
	D.5	9	8	6	3	5	75	100	100	100	100	6,75	8	6	3	5
	D. 6	5	7	6	3	6	75	100	100	100	100	3,75	7	6	3	6
	D.7	10	9	9	10	8	75	100	100	100	100	7,5	9	9	10	8
[COM]																
	COM. 1	0	3	0	0	3	50	100	75	100		0	3	0	0	0
	COM. 2	3	8	8	8	7	50	100	75	100		1,5	8	6	8	0
	COM. 3	0	0	0	2	2	50	100	75	100		0	0	0	1,5	0
	COM. 4	8	8	10	10	8	50	100	75	100		4	8	7,5	10	0
	COM. 5	0	0	0	2	0	50	100	75	100		0	0	0	2	0
[S]																
	S.1	6	8	6	8	6	100	100	100	100	25	6	8	6	8	1,25
	S.2	8	8	10	10	8	100	100	100	100	25	8	8	10	10	2
[AUX]																
	AUX. 1	0	0	0	9	0		25	100	100		0	0	0	9	0
	AUX. 2	0	0	0	8	0		25	100	100		0	0	0	8	0
	AUX. 3	0	0	0	9	0		25	100	100		0	0	0	9	0
	AUX. 4	8	8	10	10	8		25	100	100		0	2	10	10	0
	AUX. 5	0	0	0	8	0		25	100	100		0	0	0	8	0
[P]																
	P.1	7	7	7	7	7		100	75	100		0	7	5,25	7	0
	P.2	8	8	7	10	8		100	75	100		0	8	5,25	10	0
	P.3	8	8	7	9	8		100	75	100		0	8	5,25	9	0
	P.4	8	8	6	9	8		100	75	100		0	8	4,5	9	0

	P.5	8	5	2	6	3		100	75	100		0	5	1,5	6	0
	P.6	8	3	3	8	3		100	75	100		0	3	2,25	8	0

Tabla 13

3.8 Nivel de Riesgo Aceptable y Riesgo Residual

En este punto, se determinará el nivel de Riesgo Aceptable, que será el nivel por debajo del cual, un riesgo será asumido por la organización. De esta forma, una vez definido, se realizarán las propuestas de proyectos que puedan reducir los riegos superiores al Riesgo Aceptable, a valores inferiores a este, así como la definición de controles para monitorizar y asegurar la disminución de estos riesgos.

Por otro lado, el riesgo que se mantenga una vez aplicados los controles definidos, se considerará Riesgo Residual. Con estos controles, se buscará que el Riesgo Residual quede por debajo del Riesgo Aceptable.

Para calcular el Riesgo, utilizaremos los datos previamente calculados de la frecuencia de materialización de las amenazas y el impacto potencial sobre los activos. De esta forma, tendremos:

Aplicando la fórmula a los datos anteriores (redondeamos el resultado con 3 decimales), se determina la siguiente tabla:

Ámbito	ID	Frecuencia	Impacto Potencial					Riesgo				
			A	C	I	D	A	A	C	I	D	A
[L]												
	L.1	0.002739	0	10	10	10	0	0	0.027	0.027	0.027	0
	L.2	0.002739	0	10	10	10	0	0	0.027	0.027	0.027	0
[HW]												
	HW.1	0.016438	0	8	10	10	0	0	0.132	0.164	0.164	0
	HW.2	0.016438	0	8	10	10	0	0	0.132	0.164	0.164	0
	HW.3	0.016438	0	8	5	8	0	0	0.132	0.082	0.132	0
	HW.4	0.016438	0	3	3	0	0	0	0.049	0.049	0	0
	HW.5	0.016438	0	3	5	5	0	0	0.049	0.082	0.082	0
	HW.6	0.016438	0	8	8	10	0	0	0.132	0.132	0.164	0
	HW.7	0.016438	0	3	0	0	0	0	0.049	0	0	0
	HW.8	0.016438	0	0	0	0	0	0	0	0	0	0
	HW.9	0.016438	0	0	0	3	0	0	0	0	0.049	0
	HW.10	0.016438	0	3	3	10	0	0	0.049	0.049	0.164	0
	HW.11	0.016438	0	8	8	7	0	0	0.132	0.132	0.115	0
[SW]												
	SW.1	0.016438	4.5	6	8	9	0	0.074	0.099	0.132	0.148	0
	SW.2	0.016438	4.5	6	8	9	0	0.074	0.099	0.132	0.148	0
	SW.3	0.016438	3.75	8	6	8	0	0.062	0.132	0.099	0.132	0

	SW.4	0.016438	3.75	8	6	6	0	0.062	0.132	0.099	0.099	0
	SW.5	0.016438	2.25	3	5	5	0	0.037	0.049	0.082	0.082	0
	SW.6	0.016438	3.75	7	6	7	0	0.062	0.115	0.099	0.115	0
	SW.7	0.016438	3.75	5	6	7	0	0.062	0.082	0.099	0.115	0
	SW.8	0.016438	3.75	3	5	5	0	0.062	0.049	0.082	0.082	0
	SW.9	0.016438	3.75	3	5	5	0	0.062	0.049	0.082	0.082	0
	SW.10	0.016438	4.5	7	7	8	0	0.074	0.115	0.115	0.132	0
[D]												
	D.1	0.016438	6	9	9	10	8	0.099	0.148	0.148	0.164	0.132
	D.2	0.016438	6	9	9	10	8	0.099	0.148	0.148	0.164	0.132
	D.3	0.016438	3.75	6	5	8	7	0.062	0.099	0.082	0.132	0.115
	D.4	0.016438	3.75	7	7	6	7	0.016	0.115	0.115	0.099	0.115
	D.5	0.016438	6.75	8	6	3	5	0.111	0.132	0.099	0.049	0.082
	D. 6	0.016438	3.75	7	6	3	6	0.062	0.115	0.099	0.049	0.099
	D.7	0.016438	7.5	9	9	10	8	0.123	0.148	0.148	0.164	0.132
[COM]												
	COM.1	0.005479	0	3	0	0	0	0	0.016	0	0	0
	COM.2	0.005479	1.5	8	6	8	0	0.008	0.044	0.033	0.044	0
	COM.3	0.005479	0	0	0	1.5	0	0	0	0	0.008	0
	COM.4	0.005479	4	8	7.5	10	0	0.022	0.044	0.041	0.055	0
	COM.5	0.005479	0	0	0	2	0	0	0	0	0.011	0
[S]												
	S.1	0.002739	6	8	6	8	1.25	0.016	0.022	0.016	0.022	0.003
	S.2	0.002739	8	8	10	10	2	0.022	0.022	0.027	0.027	0.005
[AUX]												
	AUX.1	0.016438	0	0	0	9	0	0	0	0	0.148	0
	AUX.2	0.016438	0	0	0	8	0	0	0	0	0.132	0
	AUX.3	0.016438	0	0	0	9	0	0	0	0	0.148	0
	AUX.4	0.016438	0	2	10	10	0	0	0.033	0.164	0.164	0
	AUX.5	0.016438	0	0	0	8	0	0	0	0	0.132	0
[P]												
	P.1	0.016438	0	7	5.25	7	0	0	0.115	0.086	0.115	0
	P.2	0.016438	0	8	5.25	10	0	0	0.132	0.086	0.164	0
	P.3	0.016438	0	8	5.25	9	0	0	0.132	0.086	0.148	0
	P.4	0.016438	0	8	4.5	9	0	0	0.132	0.074	0.148	0
	P.5	0.016438	0	5	1.5	6	0	0	0.082	0.025	0.099	0
	P.6	0.016438	0	3	2.25	8	0	0	0.049	0.037	0.132	0

Tabla 14

El valor máximo de los riesgos es 0.164, por lo que la tabla de riesgos aceptables definida en la metodología quedaría con los valores:

Nivel aceptable de riesgo	Valor	Explicación
Alto	75%	Mayor o igual que 0.123
Medio	50%	Entre 0.04 y 0.123
Bajo	25%	Menor o igual que 0.04

Tabla 15

Tras la revisión de estos datos por parte de la dirección, se ha establecido un nivel de Riesgo Aceptable medio, es decir, la dirección de Ingeniería SL acepta como riesgo aceptable todos los riesgos que estén por debajo del valor 0.123. Para una mejor visión de los riesgos a reducir en la tabla, aparecen coloreados en rojo los valores altos.

3.9 Resultados

De la tabla anterior, es posible deducir varias conclusiones:

- El aspecto de seguridad de la información que más se ve afectado por la materialización de las amenazas, es el de la Disponibilidad, seguido de la Confidencialidad e Integridad.
- Los tipos de activos que, bajo la materialización de las amenazas, afectan a más aspectos de la seguridad de la información, son el Hardware, y sobre todo, los datos.

A continuación, se muestran los activos más relevantes para la empresa en cuanto al nivel de riesgo que presentan ante la materialización de las amenazas revisadas. Estos serán los activos que habrá que proteger de forma más inmediata.

Ámbito	Identificador	Activo
[HW] Equipamiento informático (hardware)		
	HW.1	Servidor
	HW.2	Estación de trabajo
	HW.3	PC de escritorio
	HW.6	Router (Fibra, Wifi, DHCP. Firewall)
	HW.10	Switch
	HW.11	Discos Backup
[SW] Software - Aplicaciones informáticas		
	SW.1	Control de versiones GIT
	SW.2	Gestión de proyectos REDMINE
	SW.3	SUSE Linux Enterprise
	SW.4	Ubuntu Linux
	SW.10	Antivirus Windows

[D] Datos / Información		
	D.1	Base de datos REDMINE
	D.2	Base de datos GIT
	D.3	Documentación compañía
	D.5	Datos clientes
	D.7	Datos Proyectos
[AUX] Equipamiento auxiliar		
	AUX.1	Equipamiento antiincencios
	AUX.2	Sistema de alarma
	AUX.3	Sistema de alimentación ininterrumpida
	AUX.4	Sistema climatización
	AUX.5	Armarios comunicaciones
[P] Personal		
	P.2	Director de Área
	P.3	Ingeniero desarrollo
	P.4	Ingeniero hardware i+d
	P.6	Contabilidad/Facturación (externo)

Tabla 16

Como resultado de los análisis realizados, podemos también resumir las amenazas más frecuentes que pueden incidir en los activos. Dado que se utilizó el valor mayor de frecuencia de cada tipo de amenaza para valorar la frecuencia de los grupos de amenazas sobre los grupos de activos, estas son las que más habrán aportado al riesgo que queremos reducir (sobre los activos más críticos ante el riesgo):

Ámbito	Amenazas más frecuentes	Explicación según MAGERIT
[HW] Equipamiento informático (hardware)		
	[I.6] Corte del suministro eléctrico	Cese de la alimentación de potencia
	[E.24] Caída del sistema por agotamiento de recursos	La carencia de recursos suficientes provoca la caída del sistema cuando la carga de trabajo es desmesurada.
	[A.24] Denegación de servicio	La carencia de recursos suficientes provoca la caída del sistema cuando la carga de trabajo es desmesurada.
[SW] Software - Aplicaciones informáticas		
	[E.21] Errores de mantenimiento / actualización de	Defectos en los procedimientos o controles de actualización del código que permiten que sigan

	programas (software)	utilizándose programas con defectos conocidos y reparados por el fabricante.
[D] Datos / Información		
	[E.3] Errores de monitorización (log)	Inadecuado registro de actividades: falta de registros, registros incompletos, registros incorrectamente fechados, registros incorrectamente atribuidos, ...
[AUX] Equipamiento auxiliar		
	[I.6] Corte del suministro eléctrico	Cese de la alimentación de potencia
[P] Personal		
	[E.28] Indisponibilidad del personal	Ausencia accidental del puesto de trabajo: enfermedad, alteraciones del orden público, guerra bacteriológica, ...

Tabla 17

4. Propuestas de proyectos

4.1 Introducción

Una vez conocido el nivel de riesgo actual de Ingeniería SL, es posible plantear los proyectos necesarios para mejorar el estado de la seguridad de la organización. Para ello, se utilizarán los datos obtenidos durante el proceso de Análisis de Riesgos. Según estos datos, podemos realizar una serie de recomendaciones generales para mejorar la gestión de la seguridad, que serán la base para los proyectos propuestos:

- Ampliar ciertos recursos hardware con el fin de reducir las paradas y caídas provocadas por la falta de recursos.
- Mejorar el sistema eléctrico o el de alimentación ininterrumpida para evitar pérdidas de disponibilidad.
- Mejorar la gestión del cambio, sobre todo en cuanto se refiere al mantenimiento del software crítico.
- Mejorar el registro de actividades, y en general, mejorar los procedimientos para evitar errores en la información y en los procesos.
- Reducir el impacto de la indisponibilidad del personal, por ejemplo, documentando procesos críticos.
- Establecer planes de continuidad.

Se realizará una cuantificación económica y temporal para la ejecución de los proyectos y se indicará la mejora que suponen en la gestión de la seguridad y los posibles efectos colaterales sobre otros elementos de la organización. Asimismo, se incluirán puntos de control para su evaluación, ya que estos proyectos, serán parte del proceso de mejora continua de la implementación del SGSI.

4.2 Propuestas de proyectos

A partir de las recomendaciones expuestas anteriormente, se han propuesto los siguientes proyectos de mejora:

Proyecto 1: Ampliación hardware Estaciones de trabajo
Proyecto 2: Adquisición de SAI
Proyecto 3: Procedimientos de actualización de software
Proyecto 4: Clasificación de registros de proyectos
Proyecto 5: Formación interna
Proyecto 6: Contrato confidencialidad.
Proyecto 7: Procedimiento de recuperación de desastres.
Proyecto 8: Implantación sistema de gestión de contraseñas
Proyecto 9: Documentación sobre roles y permisos de los administradores
Proyecto 10: Procedimiento de contratación y baja

Para cada proyecto, se establecerá un responsable de asegurar su correcta ejecución. También se definirá el plazo de ejecución de cada uno, objetivos perseguidos, la descripción del proyecto, las mejoras y posibles beneficios colaterales aportados y el método para controlar que

se ejecuta correctamente. Asimismo, se identificarán los activos afectados, los riegos que pretenden mitigarse y los controles aplicados del Anexo A de la norma ISO/IEC 27001:2013.

A continuación se muestra, a modo de resumen, un diagrama de Gantt con la planificación general de todos los proyectos:

Nombre	Fecha de inicio	Fecha de fin	Responsable
Proyecto 1: Ampliación hardware Estaciones de trabajo	30/04/18	29/05/18	Director área Termosolar
Proyecto 2: Adquisición de SAI	30/04/18	29/05/18	Director área Termosolar
Proyecto 3: Procedimientos de actualización de software	1/05/18	2/07/18	Director área Termosolar
Proyecto 4: Clasificación de registros de proyectos	2/04/18	3/10/18	Director área Ferrocarril
Proyecto 5: Formación interna	2/04/18	5/04/19	Director área Ferrocarril
Proyecto 6: Contrato confidencialidad	2/04/18	1/05/18	Director Ingeniería SL
Proyecto 7: Procedimiento de recuperación de desastres	30/05/18	29/06/18	Director área Termosolar
Proyecto 8: Implantación sistema de gestión de contraseñas	3/07/18	31/08/18	Director área Termosolar
Proyecto 9: Documentación sobre roles y gestión de permisos de los administradores	2/07/18	1/01/19	Director área Termosolar
Proyecto 10: Procedimiento de contratación y baja	2/05/18	3/07/18	Director Ingeniería SL

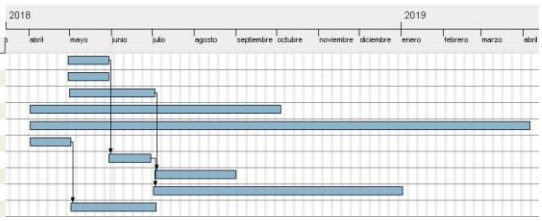


Ilustración 4

La descripción y características de estos se encuentra en el Anexo VIII.

4.3 Resultados

Una vez ejecutados con éxito los proyectos propuestos, se debe de realizar un nuevo análisis de impacto sobre la seguridad que refleje la evolución del riesgo e impacto de materialización y el nivel de cumplimiento respecto a la norma.

4.3.1 Evolución del riesgo tras la ejecución de los proyectos

Para ver la evolución del riesgo e impacto, tendrá que calcularse de nuevo el porcentaje de impacto sobre cada tipo de activo:

Ámbito	ID	Valoración					Porcentaje de impacto (%)					Impacto Potencial				
		A	C	I	D	A	A	C	I	D	A	A	C	I	D	A
[L]																
	L.1	8	10	10	10	8		100	100	75		0	10	10	7,5	0
	L.2	8	10	10	10	8		100	100	75		0	10	10	7,5	0
[HW]																
	HW.1	8	8	10	10	8		75	50	50		0	6	5	5	6
	HW.2	8	8	10	10	5		75	50	50		0	6	5	5	
	HW.3	3	8	5	8	5		75	75	75		0	6	3.75	6	3.75
	HW.4	3	3	3	0	0		75	75	75		0	2.25	2.25	0	0
	HW.5	3	3	5	5	3		75	75	75		0	2.25	3.75	3.75	2.25
	HW.6	8	8	8	10	3		75	75	50		0	6	6	5	2.25
	HW.7	3	3	0	0	0		75	75	75		0	2.25	0	0	0
	HW.8	0	0	0	0	0		75	75	75		0	0	0	0	0
	HW.9	0	0	0	3	0		75	75	75		0	0	0	2.25	0
	HW.10	3	3	3	10	3		75	75	50		0	2.25	2.25	5	2.25
	HW.11	6	8	8	7	5		75	75	75		0	6	6		3.75
[SW]																
	SW.1	6	6	8	9	6	75	75	75	50		4.5	4.5	6	4.5	0

	SW.2	6	6	8	9	6	75	75	75	50		4.5	4.5	6	4.5	0
	SW.3	5	8	6	8	5	75	75	75	50		3.75	6	4.5	4	0
	SW.4	5	8	6	6	3	75	75	75	50		3.75	6	4.5	3	0
	SW.5	3	3	5	5	3	75	75	75	50		2.25	2.25	3.75	2.5	0
	SW.6	5	7	6	7	3	75	75	75	50		3.75	5.25	4.5	3.5	0
	SW.7	5	5	6	7	3	75	75	75	50		3.75	3.75	4.5	3.5	0
	SW.8	5	3	5	5	3	75	75	75	50		3.75	2.25	3.75	2.5	0
	SW.9	5	3	5	5	3	75	75	75	50		3.75	2.25	3.75	2.5	0
	SW.10	6	7	7	8	6	75	75	75	50		4.5	5.25	5.25	4	0
[D]																
	D.1	8	9	9	10	8	75	75	75	50	75	6	6.75	6.75	5	6
	D.2	8	9	9	10	8	75	75	75	50	75	6	6.75	6.75	5	6
	D.3	5	6	5	8	7	75	75	75	50	75	3.75	4.5	3.75	4	5.25
	D.4	5	7	7	6	7	75	75	75	50	75	3.75	5.25	5.25	3	5.25
	D.5	9	8	6	3	5	75	75	75	50	75	6.75	6	4.5	1.5	3.75
	D. 6	5	7	6	3	6	75	75	75	50	75	3.75	5.25	4.5	1	4.5
	D.7	10	9	9	10	8	75	75	75	50	75	7.5	6.75	6.75	5	6
[COM]																
	COM.1	0	3	0	0	3	50	100	75	100		0	3	0	0	0
	COM.2	3	8	8	8	7	50	100	75	100		1,5	8	6	8	0
	COM.3	0	0	0	2	2	50	100	75	100		0	0	0	1,5	0
	COM.4	8	8	10	10	8	50	100	75	100		4	8	7,5	10	0
	COM.5	0	0	0	2	0	50	100	75	100		0	0	0	2	0
[S]																
	S.1	6	8	6	8	6	100	100	100	100	25	6	8	6	8	1.5
	S.2	8	8	10	10	8	100	100	100	100	25	8	8	10	10	2
[AUX]																
	AUX.1	0	0	0	9	0		25	50	50		0	0	0	4.5	0
	AUX.2	0	0	0	8	0		25	50	50		0	0	0	4	0
	AUX.3	0	0	0	9	0		25	50	50		0	0	0	4.5	0
	AUX.4	8	8	10	10	8		25	50	50		0	2	5	5	0
	AUX.5	0	0	0	8	0		25	50	50		0	0	0	4	0
[P]																
	P.1	7	7	7	7	7		50	50	50		0	3.5	3.5	3.5	0
	P.2	8	8	7	10	8		50	50	50		0	4	3.5	5	0
	P.3	8	8	7	9	8		50	50	50		0	4	3.5	4.5	0
	P.4	8	8	6	9	8		50	50	50		0	4	3	4.5	0
	P.5	8	5	2	6	3		50	50	50		0	2.5	1	3	0
	P.6	8	3	3	8	3		50	50	50		0	1.5	1.5	4	0

Tabla 18

Con los nuevos valores, ya es posible calcular el nuevo valor de riesgo:

Ámbito	ID	Frecuencia	Impacto Potencial					Riesgo				
			A	C	I	D	A	A	C	I	D	A
[L]												

	L.1	0.002739	0	10	10	7,5	0	0	0.027	0.027	0.003	0
	L.2	0.002739	0	10	10	7,5	0	0	0.027	0.027	0.003	0
								0	0	0	0	0
[HW]								0	0	0	0	0
	HW.1	0.016438	0	6	5	5	6	0	0.099	0.082	0.082	0.099
	HW.2	0.016438	0	6	5	5		0	0.099	0.082	0.082	0.016
	HW.3	0.016438	0	6	3.75	6	3.75	0	0.099	0.062	0.099	0.062
	HW.4	0.016438	0	2.25	2.25	0	0	0	0.037	0.037	0	0
	HW.5	0.016438	0	2.25	3.75	3.75	2.25	0	0.037	0.062	0.062	0.037
	HW.6	0.016438	0	6	6	5	2.25	0	0.099	0.099	0.082	0.037
	HW.7	0.016438	0	2.25	0	0	0	0	0.037	0	0	0
	HW.8	0.016438	0	0	0	0	0	0	0	0	0	0
	HW.9	0.016438	0	0	0	2.25	0	0	0	0	0.037	0
	HW.10	0.016438	0	2.25	2.25	5	2.25	0	0.037	0.037	0.082	0.037
	HW.11	0.016438	0	6	6		3.75	0	0.099	0.099	0.016	0.062
								0	0	0	0	0
[SW]								0	0	0	0	0
	SW.1	0.016438	4.5	4.5	6	4.5	0	0.074	0.074	0.099	0.074	0
	SW.2	0.016438	4.5	4.5	6	4.5	0	0.074	0.074	0.099	0.074	0
	SW.3	0.016438	3.75	6	4.5	4	0	0.062	0.099	0.074	0.066	0
	SW.4	0.016438	3.75	6	4.5	3	0	0.062	0.099	0.074	0.049	0
	SW.5	0.016438	2.25	2.25	3.75	2.5	0	0.037	0.037	0.062	0.041	0
	SW.6	0.016438	3.75	5.25	4.5	3.5	0	0.062	0.086	0.074	0.058	0
	SW.7	0.016438	3.75	3.75	4.5	3.5	0	0.062	0.062	0.074	0.058	0
	SW.8	0.016438	3.75	2.25	3.75	2.5	0	0.062	0.037	0.062	0.041	0
	SW.9	0.016438	3.75	2.25	3.75	2.5	0	0.062	0.037	0.062	0.041	0
	SW.10	0.016438	4.5	5.25	5.25	4	0	0.074	0.086	0.086	0.066	0
								0	0	0	0	0
[D]								0	0	0	0	0
	D.1	0.016438	6	6.75	6.75	5	6	0.099	0.111	0.111	0.082	0.099
	D.2	0.016438	6	6.75	6.75	5	6	0.099	0.111	0.111	0.082	0.099
	D.3	0.016438	3.75	4.5	3.75	4	5.25	0.062	0.074	0.062	0.066	0.086
	D.4	0.016438	3.75	5.25	5.25	3	5.25	0.062	0.086	0.086	0.049	0.086
	D.5	0.016438	6.75	6	4.5	1.5	3.75	0.111	0.099	0.074	0.025	0.062
	D. 6	0.016438	3.75	5.25	4.5	1	4.5	0.062	0.086	0.074	0.016	0.074
	D.7	0.016438	7.5	6.75	6.75	5	6	0.123	0.111	0.111	0.082	0.099
								0	0	0	0	0
[COM]								0	0	0	0	0
	COM.1	0.005479	0	3	0	0	0	0	0.016	0	0	0
	COM.2	0.005479	1,5	8	6	8	0	0.005	0.044	0.033	0.044	0
	COM.3	0.005479	0	0	0	1,5	0	0	0	0	0.005	0
	COM.4	0.005479	4	8	7,5	10	0	0.022	0.044	0.005	0.055	0
	COM.5	0.005479	0	0	0	2	0	0	0	0	0.011	0
								0	0	0	0	0
[S]								0	0	0	0	0
	S.1	0.002739	6	8	6	8	1.5	0.016	0.022	0.016	0.022	0.004
	S.2	0.002739	8	8	10	10	2	0.022	0.022	0.027	0.027	0.005
								0	0	0	0	0
[AUX]								0	0	0	0	0

	AUX.1	0.016438	0	0	0	4.5	0	0	0	0	0.074	0
	AUX.2	0.016438	0	0	0	4	0	0	0	0	0.066	0
	AUX.3	0.016438	0	0	0	4.5	0	0	0	0	0.074	0
	AUX.4	0.016438	0	2	5	5	0	0	0.033	0.082	0.082	0
	AUX.5	0.016438	0	0	0	4	0	0	0	0	0.066	0
								0	0	0	0	0
[P]								0	0	0	0	0
	P.1	0.016438	0	3.5	3.5	3.5	0	0	0.058	0.058	0.058	0
	P.2	0.016438	0	4	3.5	5	0	0	0.066	0.058	0.082	0
	P.3	0.016438	0	4	3.5	4.5	0	0	0.066	0.058	0.074	0
	P.4	0.016438	0	4	3	4.5	0	0	0.066	0.049	0.074	0
	P.5	0.016438	0	2.5	1	3	0	0	0.041	0.016	0.049	0
	P.6	0.016438	0	1.5	1.5	4	0	0	0.025	0.025	0.066	0

Tabla 19

Como se puede ver en la tabla anterior, una vez realizados con éxito los proyectos, el nivel de riesgo para cada activo, está por debajo del valor acordado (0.123) como riesgo aceptable.

4.3.1 Nivel de cumplimiento respecto a la norma

Se vuelve a realizar un análisis diferencial respecto a los dominios de la norma ISO/IEC 27002:

Controles	Valoración
5. POLITICAS DE SEGURIDAD	
5.1 Directrices de la Dirección en seguridad de la información.	
5.1.1 Conjunto de políticas para la seguridad de la información.	L3
5.1.2 Revisión de las políticas para la seguridad de la información.	L3
6. ASPECTOS ORGANIZATIVOS DE LA SEGURIDAD DE LA INFORMACION	
6.1 Organización interna.	
6.1.1 Asignación de responsabilidades para la segur. de la información.	L3
6.1.2 Segregación de tareas.	L1
6.1.3 Contacto con las autoridades.	L2
6.1.4 Contacto con grupos de interés especial.	L1
6.1.5 Seguridad de la información en la gestión de proyectos.	L3
6.2 Dispositivos para movilidad y teletrabajo.	
6.2.1 Política de uso de dispositivos para movilidad.	L3
6.2.2 Teletrabajo.	L1
7. SEGURIDAD LIGADA A LOS RECURSOS HUMANOS	
7.1 Antes de la contratación.	
7.1.1 Investigación de antecedentes.	L3
7.1.2 Términos y condiciones de contratación.	L3
7.2 Durante el empleo.	
7.2.1 Responsabilidades de gestión.	L3
7.2.2 Concienciación, educación y capacitación en seguridad de la información.	L3
7.2.3 Proceso disciplinario.	L3
7.3 Finalización de empleo o cambio de puesto de trabajo.	
7.3.1 Responsabilidades ante la finalización o cambio	L3
8. GESTION DE ACTIVOS	
8.1 Responsabilidad sobre los activos.	
8.1.1 Inventario de activos.	L3

8.1.2 Propiedad de los activos.	L2
8.1.3 Uso aceptable de los activos.	L2
8.1.4 Devolución de activos.	L2
8.2 Clasificación de la información.	
8.2.1 Directrices de clasificación.	L3
8.2.2 Etiquetado y manipulado de la información.	L3
8.2.3 Manipulado de la información	L3
8.3 Manipulación de los soportes	
8.3.1 Gestión de soportes extraíbles.	L3
8.3.2 Eliminación de soportes.	L1
8.3.3 Soportes físicos en tránsito.	L3
9. CONTROL DE ACCESOS	
9.1 Requisitos de negocio para el control de accesos.	
9.1.1 Política de control de accesos.	L3
9.1.2 Acceso a las redes y a los servicios de red	L3
9.2 Gestión de acceso de usuario.	
9.2.1 Registro y baja de usuario.	L3
9.2.2 Provisión de acceso de usuario.	L3
9.2.3 Gestión de los derechos de acceso con privilegios especiales.	L3
9.2.4 Gestión de información secreta de autenticación de usuarios.	L3
9.2.5 Revisión de los derechos de acceso de usuario.	L1
9.2.6 Retirada o adaptación de los derechos de acceso	L3
9.3 Responsabilidades del usuario.	
9.3.1 Uso de información secreta para la autenticación.	L2
9.4 Control de acceso a sistemas y aplicaciones.	
9.4.1 Restricción del acceso a la información.	L2
9.4.2 Procedimientos seguros de inicio de sesión.	L2
9.4.3 Sistema de gestión de contraseñas.	L3
9.4.4 Uso de utilidades con privilegios de sistemas.	L1
9.4.5 Control de acceso al código fuente de los programas.	L2
10. CRIPTOGRAFIA	
10.1 Controles criptográficos.	
10.1.1 Política de uso de los controles criptográficos.	L0
10.1.2 Gestión de claves.	L0
11. SEGURIDAD FISICA Y AMBIENTAL	
11.1 Áreas seguras.	
11.1.1 Perímetro de seguridad física.	L1
11.1.2 Controles físicos de entrada.	L2
11.1.3 Seguridad de oficinas, despachos y recursos.	L1
11.1.4 Protección contra las amenazas externas y ambientales.	L1
11.1.5 El trabajo en áreas seguras.	L2
11.1.6 Áreas de acceso público, carga y descarga.	N/A
11.2 Seguridad de los equipos.	
11.2.1 Emplazamiento y protección de equipos.	L1
11.2.2 Instalaciones de suministro.	L1
11.2.3 Seguridad del cableado.	L2
11.2.4 Mantenimiento de los equipos.	L2
11.2.5 Retirada de materiales propiedad de la empresa	L1
11.2.6 Seguridad de los equipos y activos fuera de las instalaciones.	L2
11.2.7 Reutilización o retirada segura de dispositivos de equipos.	L1
11.2.8 Equipo de usuario desatendido.	L0
11.2.9 Política de puesto de trabajo despejado y bloqueo de pantalla.	L3
12. SEGURIDAD EN LAS OPERACIONES	
12.1 Procedimientos y responsabilidades operacionales.	
12.1.1 Documentación de procedimientos de operación.	L3

12.1.2 Gestión de cambios.	L3
12.1.3 Gestión de capacidades.	L2
12.1.4 Separación de los recursos de desarrollo, prueba y producción.	L2
12.2 Protección contra código malicioso.	
12.2.1 Controles contra el código malicioso.	L3
12.3 Copias de seguridad.	
12.3.1 Copias de seguridad de la información.	L3
12.4 Registros y supervisión.	
12.4.1 Registro de eventos	L3
12.4.2 Protección de la información de registro.	L3
12.4.3 Registros de administración y operación.	L1
12.4.4 Sincronización de relojes.	L1
12.5 Control del software en explotación.	
12.5.1 Instalación del software en sistemas en producción.	L2
12.6 Gestión de la vulnerabilidad técnica.	
12.6.1 Gestión de las vulnerabilidades técnicas.	L3
12.6.2 Restricciones en la instalación de software.	L2
12.7 Consideraciones de las auditorias de los sistemas de información.	
12.7.1 Controles de auditoria de los sistemas de información.	L3
13. SEGURIDAD EN LAS TELECOMUNICACIONES	
13.1 Gestión de la seguridad de redes.	
13.1.1 Controles de red.	L1
13.1.2 Seguridad de los servicios en red.	L0
13.1.3 Segregación en redes.	L0
13.2 Intercambio de información	
13.2.1 Políticas y procedimientos de intercambio de información.	L0
13.2.2 Acuerdos de intercambio de información.	L0
13.2.3 Mensajería electrónica.	L0
13.2.4 Acuerdos de confidencialidad o no revelación	L1
14. ADQUISICION, DESARROLLO Y MANTENIMIENTO DE LOS SISTEMAS DE INFORMACION	
14.1 Requisitos de seguridad en sistemas de información.	
14.1.1 Análisis de requisitos y especificaciones de seguridad de la información.	L0
14.1.2 Asegurar los servicios de aplicaciones en redes públicas.	L1
14.1.3 Protección de las transacciones de servicios de aplicaciones.	L1
14.2 Seguridad en los procesos de desarrollo y soporte.	
14.2.1 Política de desarrollo seguro de software.	L0
14.2.2 Procedimientos de control de cambios en los sistemas.	L3
14.2.3 Revisión técnica de las aplicaciones tras efectuar cambios en el sistema operativo	L3
14.2.4 Restricciones a los cambios en los paquetes de software.	L3
14.2.5 Uso de principios de ingeniería en protección de sistemas.	L1
14.2.6 Seguridad en entornos de desarrollo.	L2
14.2.7 Externalización del desarrollo de software.	L3
14.2.8 Pruebas de funcionalidad durante el desarrollo de los sistemas.	L1
14.2.9 Pruebas de aceptación.	L1
14.3 Datos de prueba.	
14.3.1 Protección de los datos utilizados en pruebas.	L1
15. RELACIONES CON SUMINISTRADORES	
15.1 Seguridad de la información en las relaciones con suministradores.	
15.1.1 Política de seguridad de la información para suministradores.	L0
15.1.2 Tratamiento del riesgo dentro de acuerdos de suministradores.	L0
15.1.3 Cadena de suministro en tecnologías de la información y comunicaciones	L0
15.2 Gestión de la prestación del servicio por suministradores.	
15.2.1 Supervisión y revisión de los servicios prestados por terceros.	L1
15.2.2 Gestión de cambios en los servicios prestados por terceros.	L1

16. GESTION DE INCIDENTES EN LA SEGURIDAD DE LA INFORMACION	
16.1 Gestión de incidentes de seguridad de la información y mejoras.	
16.1.1 Responsabilidades y procedimientos.	L3
16.1.2 Notificación de los eventos de seguridad de la información.	L1
16.1.3 Notificación de puntos débiles de la seguridad.	L0
16.1.4 Valoración de eventos de seguridad de la información y toma de decisiones	L0
16.1.5 Respuesta a los incidentes de seguridad.	L1
16.1.6 Aprendizaje de los incidentes de seguridad de la información.	L1
16.1.7 Recopilación de evidencias.	L0
17. ASPECTOS DE SEGURIDAD DE LA INFORMACION EN LA GESTION DE LA CONTINUIDAD DE NEGOCIO	
17.1 Continuidad de la seguridad de la información.	
17.1.1 Planificación de la continuidad de la seguridad de la información.	L3
17.1.1 Planificación de la continuidad de la seguridad de la información.	L3
17.1.3 Verificación, revisión y evaluación de la continuidad de la seguridad de la información	L3
17.2 Redundancias	
17.2.1 Disponibilidad de instalaciones para el procesamiento de la información	L0
18. CUMPLIMIENTO	
18.1 Cumplimiento de los requisitos legales y contractuales	
18.1.1 Identificación de la legislación aplicable.	L1
18.1.2 Derechos de propiedad intelectual (DPI).	L2
18.1.3 Protección de los registros de la organización.	L2
18.1.4 Protección de datos y privacidad de la información personal.	L2
18.1.5 Regulación de los controles criptográficos.	L1
18.2 Revisiones de la seguridad de la información.	
18.2.1 Revisión independiente de la seguridad de la información.	L1
18.2.2 Cumplimiento de las políticas y normas de seguridad.	L3
18.2.3 Comprobación del cumplimiento.	L3

Tabla 20

El resumen por dominio de la gráfica anterior quedaría:

Dominio	**Conformidad (%)**
5. Políticas de Seguridad	90
6. Aspectos Organizativos de la Seguridad de la Información	50
7. Seguridad ligada a los recursos humanos	90
8. Gestión de activos	71
9. Control de accesos	66.67
10. Criptografía	0
11. Seguridad Física y ambiental	57.11
12. Seguridad en las operaciones	72.8
13. Seguridad en las telecomunicaciones	2.9
14. Adquisición, desarrollo y mantenimiento de los sistemas de información	21.8
15. Relaciones con suministradores	5
16. Gestión de incidentes en la seguridad de la información	17.1
17. Aspectos de seguridad de la información en la gestión de la continuidad de negocio	45
18. Cumplimiento	48.66

Tabla 21

Una vez obtenida una nueva valoración de los dominios de la norma, a continuación, se muestra la gráfica comparativa entre el estado inicial y el estado tras la ejecución con éxito de los proyectos planteados:

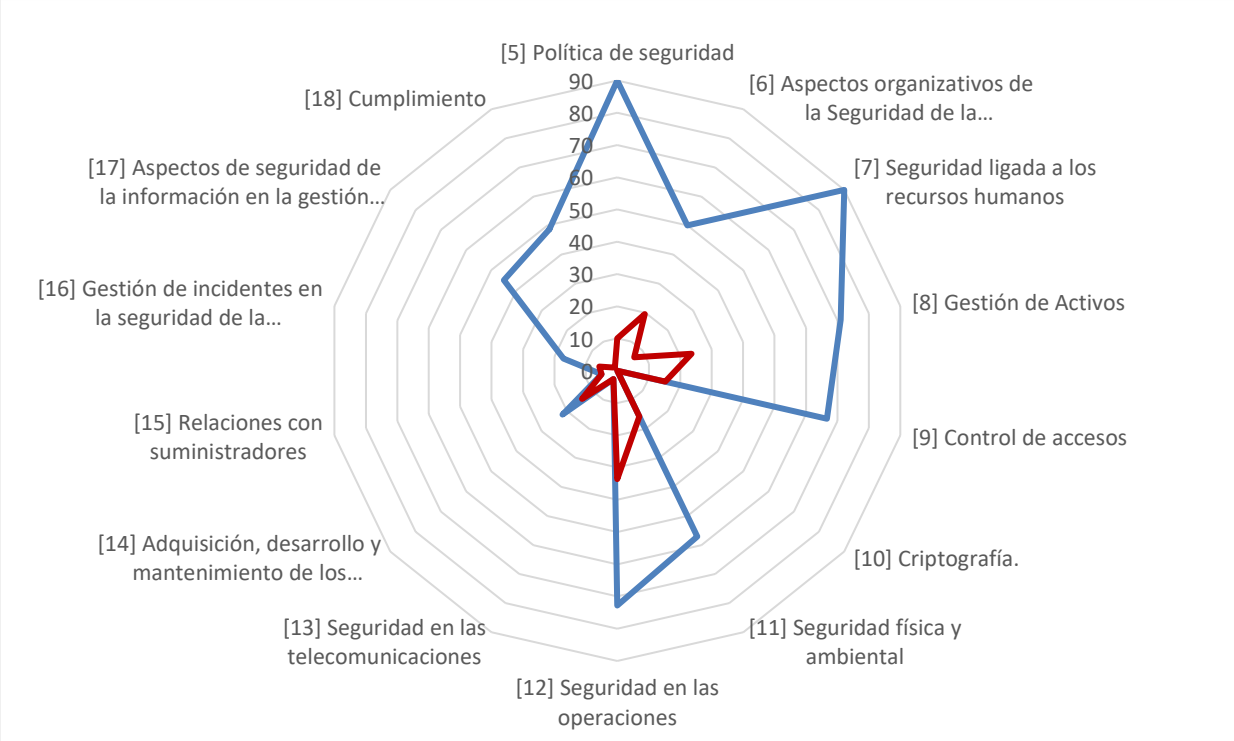


Ilustración 5

Puede verse claramente la diferencia y mejora entre los datos iniciales de cumplimiento (línea azul) y los valores una vez realizadas las mejoras (línea roja), aunque claramente, hay mucho por mejorar. Sin embargo, en los objetivos de este proyecto, ya se avanzó que se pretendía mejorar algunos aspectos de la seguridad de la información y no se buscaba inicialmente la certificación en la norma. El proyecto está sirviendo para sentar las bases de una correcta gestión de la seguridad de la información.

5. Auditoría de Cumplimiento

5.1 Introducción

Durante las fases anteriores del proyecto, se han identificado en su totalidad los activos de la empresa, se han evaluado las amenazas. También se ha generado la documentación base del SGSI y se han definido e implantado proyectos de mejora en la organización. En este punto, es el momento de evaluar el nivel de madurez de la seguridad de la información en la organización, en referencia a los requisitos definidos en los apartados 4 al 10 de la ISO/IEC 2001/2013. Uno de esos requisitos, corresponde al análisis de riesgos ya realizado, por lo que se evaluarán también los controles del anexo A, detallados en la ISO/IEC 2002/2013.

5.2 Metodología

Se evaluarán los requerimientos definidos en la norma ISO/IEC 2001/2013, así como los controles de la ISO/UEC 27002/2013.

Para realizar esta evaluación, se utilizará como metodología el modelo de madurez de la capacidad (CMM). Mediante este método, se revisará la efectividad de los controles de la norma en cada dominio, utilizando la tabla de valores definida previamente en el apartado 1.5:

EFECTIVIDAD	CMM	SIGNIFICADO	DESCRIPCIÓN
0%	**L0**	Inexistente	Carencia completa de cualquier proceso reconocible. No se ha reconocido siquiera que existe un problema a resolver.
10%	**L1**	Inicial / Ad-hoc	Estado inicial donde el éxito de las actividades de los procesos se basa la mayoría de las veces en el esfuerzo personal. Los procedimientos son inexistentes o localizados en áreas concretas. No existen plantillas definidas a nivel corporativo.
50%	**L2**	Reproducible, pero intuitivo	Los procesos similares se llevan en forma similar por diferentes personas con la misma tarea. Se normalizan las buenas prácticas en base a la experiencia y al método. No hay comunicación o entrenamiento formal, las responsabilidades quedan a cargo de cada individuo. Se depende del grado de conocimiento de cada individuo.
90%	**L3**	Proceso definido	La organización entera participa en el proceso. Los procesos están implantados, documentados y comunicados mediante entrenamiento.

95%	**L4**	Gestionado y medible	Se puede seguir con indicadores numéricos y estadísticos la evolución de los procesos. Se dispone de tecnología para automatizar el flujo de trabajo, se tienen herramientas para mejorar la calidad y la eficiencia.
100%	**L5**	Optimizado	Los procesos están bajo constante mejora. En base a criterios cuantitativos se determinan las desviaciones más comunes y se optimizan los procesos.

Tabla 22

5.3 Alcance

Para la evaluación de la madurez, se analizarán los siguientes apartados de la norma ISO/IEC 27001/2013:

4.- Contexto de la organización
5.- Liderazgo
6.- Planificación
7.- Soporte
8.- Operación
9.- Evaluación del desempeño
10.- Mejora

Además, como requerimiento del apartado 6, se auditarán también los controles de los dominios de la norma ISO/IEC 27002/2013:

[5] Política de seguridad
[6] Aspectos organizativos de la Seguridad de la Información.
[7] Seguridad ligada a los recursos humanos.
[8] Gestión de activos
[9] Control de accesos
[10] Criptografía
[11] Seguridad física y ambiental
[12] Seguridad en las operaciones
[13] Seguridad en las Telecomunicaciones
[14] Adquisición, desarrollo y mantenimiento de los sistemas de información
[15] Relaciones con suministradores
[16] Gestión de incidentes en la seguridad de la información.
[17] Aspectos de seguridad de la información en la gestión de la continuidad de negocio.
[18] Cumplimiento

5.4 Evaluación de la Madurez

Se muestra a continuación, la evaluación para cada apartado de la norma ISO/IEC 27001/2013:

4.CONTEXTO DE LA ORGANIZACIÓN	
4.1 Comprensión de la organización y de su contexto	L3
4.2 Comprensión de las necesidades y expectativas de las partes interesadas	L3

4.3 Determinación del alcance del SGSI	L3
4.4 SGSI	L3
5. LIDERAZGO	
5.1 Liderazgo y compromiso	L3
5.2 Política	L3
5.3 Roles, responsabilidades y autoridades en la organización	L3
6. PLANIFICACIÓN	
6.1 Acciones para hacer frente a los riesgos y oportunidades	
6.1.1 General	L3
6.1.2 Valoración de los riesgos de seguridad de la información	L3
6.1.3 Tratamiento de los riesgos de seguridad de la información	L3
6.2 Objetivos de seguridad de la información y planificación para conseguirlos	L3
7. SOPORTE	
7.1 Recursos	L3
7.2 Competencia	L2
7.3 Concienciación	L3
7.4 Comunicación	L2
7.5 Información documentada	
7.5.1 General	L3
7.5.2 Creando y actualizando	L2
7.5.3 Control de la información documentada	L3
8. OPERACIÓN	
8.1 Planificación y control	L3
8.2 Valoración de los riesgos de la seguridad de la información	L3
8.3 Tratamiento de los riesgos de la seguridad de la información	L3
9. EVALUACIÓN DEL DESEMPEÑO	
9.1 Seguimiento, medición, análisis y evaluación	L3
9.2 Auditoría interna	L3
9.3 Revisión por la dirección	L3
10. MEJORA	
10.1 No conformidad y acciones correctivas	L2
10.2 Mejora continua	L3

Tabla 23

A continuación, se muestra, para cada dominio de ISO/IEC 27002/2013, los objetivos de control que cubre y la evaluación de la madurez de cada control, entre la fase inicial del proyecto y el momento actual:

[5] Política de seguridad

Objetivo1: Dirigir y dar soporte a la gestión de la seguridad de la información en concordancia con los requerimientos del negocio, las leyes y las regulaciones.

Control	Valoración inicial	Valoración final
[5] Política de seguridad	10%	90%
[5.1] Directrices de la Dirección en seguridad de la información.		
[5.1.1] Conjunto de políticas para la seguridad de la información.	L1	L3
[5.1.2] Revisión de las políticas para la seguridad de la información.	L1	L3

Tabla 24

[6] Aspectos organizativos de la Seguridad de la Información

Objetivo1: Establecer un esquema directivo de gestión para iniciar y controlar la implementación y operativa de la seguridad de la información en la organización.

Objetivo2: Garantizar la seguridad de la información en el uso de recursos de informática móvil y teletrabajo.

Control	Valoración inicial	Valoración final
[6] Aspectos organizativos de la Seguridad de la Información	19.5%	50%
6.1 Organización interna.		
6.1.1 Asignación de responsabilidades para la seguridad de la información.	L2	L3
6.1.2 Segregación de tareas.	L1	L1
6.1.3 Contacto con las autoridades.	L2	L2
6.1.4 Contacto con grupos de interés especial.	L1	L1
6.1.5 Seguridad de la información en la gestión de proyectos.	L2	L3
6.2 Dispositivos para movilidad y teletrabajo.		
6.2.1 Política de uso de dispositivos para movilidad.	L0	L3
6.2.2 Teletrabajo.	L1	L1

Tabla 25

[7] Seguridad ligada a los recursos humanos

Objetivo1: Asegurar que los empleados, contratistas y usuarios de terceras partes entiendan sus responsabilidades y sean aptos para las funciones que desarrollen. Reducir el riesgo de robo, fraude y mal uso de las instalaciones y medios.

Objetivo2: Asegurarse de que los empleados y contratistas están en conocimiento y cumplen con sus responsabilidades en seguridad de la información.

Objetivo3: Proteger los intereses de la organización durante el proceso de cambio o finalización de empleo por parte de empleados y contratistas.

Control	Valoración inicial	Valoración final
[7] Seguridad ligada a los recursos humanos	5.5%	90%
7.1 Antes de la contratación.		
7.1.1 Investigación de antecedentes.	L0	L3
7.1.2 Términos y condiciones de contratación.	L0	L3
7.2 Durante el empleo.		
7.2.1 Responsabilidades de gestión.	L1	L3
7.2.2 Concienciación, educación y capacitación en seguridad de la información.	L2	L3
7.2.3 Proceso disciplinario.	L0	L3
7.3 Finalización de empleo o cambio de puesto de trabajo.		
7.3.1 Responsabilidades ante la finalización o cambio	L0	L3

Tabla 26

[8]. Gestión de activos

Objetivo1: Identificar los activos en la organización y definir las responsabilidades para una protección adecuada.

Objetivo2: Asegurar que se aplica un nivel de protección adecuado a la información.

Objetivo3: Evitar la divulgación, modificación, retirada o destrucción de activos no autorizada almacenada en soportes de almacenamiento.

Control	Valoración inicial	Valoración final
[8] Gestión de Activos	23.6%	71.11%
8.1 Responsabilidad sobre los activos.		
8.1.1 Inventario de activos.	L2	L3
8.1.2 Propiedad de los activos.	L2	L2
8.1.3 Uso aceptable de los activos.	L0	L2
8.1.4 Devolución de activos.	L1	L2
8.2 Clasificación de la información.		
8.2.1 Directrices de clasificación.	L2	L3
8.2.2 Etiquetado y manipulado de la información.	L2	L3
8.2.3 Manipulado de la información	L1	L3
8.3 Manipulación de los soportes		
8.3.1 Gestión de soportes extraíbles.	L1	L3
8.3.2 Eliminación de soportes.	L1	L1
8.3.3 Soportes físicos en tránsito.	L0	L3

Tabla 27

[9]. Control de accesos

Objetivo1: Controlar los accesos a la información y las instalaciones utilizadas para su procesamiento.

Objetivo2: Garantizar el acceso a los usuarios autorizados e impedir los accesos no autorizados a los sistemas de información y servicios.

Objetivo3: Hacer que los usuarios sean responsables de la protección de la información para su identificación.

Objetivo4: Impedir el acceso no autorizado a la información mantenida por los sistemas y aplicaciones.

Control	Valoración inicial	Valoración final
[9] Control de accesos	15.16%	66.67%
9.1 Requisitos de negocio para el control de accesos.		
9.1.1 Política de control de accesos.	L1	L3
9.1.2 Acceso a las redes y a los servicios de red	L0	L3
9.2 Gestión de acceso de usuario.		
9.2.1 Registro y baja de usuario.	L1	L3
9.2.2 Provisión de acceso de usuario.	L2	L3
9.2.3 Gestión de los derechos de acceso con privilegios especiales.	L1	L3
9.2.4 Gestión de información secreta de autenticación de usuarios.	L1	L3

9.2.5 Revisión de los derechos de acceso de usuario.	L0	L1
9.2.6 Retirada o adaptación de los derechos de acceso	L2	L3
9.3 Responsabilidades del usuario.		
9.3.1 Uso de información secreta para la autenticación.	L1	L2
9.4 Control de acceso a sistemas y aplicaciones.		
9.4.1 Restricción del acceso a la información.	L2	L2
9.4.2 Procedimientos seguros de inicio de sesión.	L1	L2
9.4.3 Sistema de gestión de contraseñas.	L0	L3
9.4.4 Uso de utilidades con privilegios de sistemas.	L1	L1
9.4.5 Control de acceso al código fuente de los programas.	L2	L2

Tabla 28

[10] Criptografía.

Objetivo1: Garantizar un uso adecuado y eficaz de la criptografía para proteger la confidencialidad, la autenticidad y/o la integridad de la información.

Control	Valoración inicial	Valoración final
[10] Criptografía.	0%	0%
10.1 Controles criptográficos.		
10.1.1 Política de uso de los controles criptográficos.	L0	L0
10.1.2 Gestión de claves.	L0	L0

Tabla 29

[11] Seguridad física y ambiental

Objetivo1: Evitar el acceso físico no autorizado, los daños e interferencias a la información de la organización y las instalaciones de procesamiento de la información

Objetivo2: Evitar la pérdida, los daños, el robo o el compromiso de activos y la interrupción a las operaciones de la organización.

Control	Valoración inicial	Valoración final
[11] Seguridad física y ambiental	15.17%	57.11%
11.1 Áreas seguras.		
11.1.1 Perímetro de seguridad física.	L1	L1
11.1.2 Controles físicos de entrada.	L2	L2
11.1.3 Seguridad de oficinas, despachos y recursos.	L1	L1
11.1.4 Protección contra las amenazas externas y ambientales.	L1	L1
11.1.5 El trabajo en áreas seguras.	L0	L2
11.1.6 Áreas de acceso público, carga y descarga.	N/A	N/A
11.2 Seguridad de los equipos.		
11.2.1 Emplazamiento y protección de equipos.	L1	L1
11.2.2 Instalaciones de suministro.	L1	L1
11.2.3 Seguridad del cableado.	L2	L2
11.2.4 Mantenimiento de los equipos.	L2	L2
11.2.5 Retirada de materiales propiedad de la empresa	L1	L1
11.2.6 Seguridad de los equipos y activos fuera de las instalaciones.	L0	L2
11.2.7 Reutilización o retirada segura de dispositivos de equipos.	L1	L1
11.2.8 Equipo de usuario desatendido.	L0	L0
11.2.9 Política de puesto de trabajo despejado y bloqueo de pantalla.	L0	L3

Tabla 30

[12] Seguridad en las operaciones

Objetivo1: Evitar el acceso físico no autorizado, los daños e interferencias a la información de la organización y las instalaciones de procesamiento de la información.

Objetivo2: Garantizar que la información y las instalaciones de procesamiento de información estén protegidas contra el malware

Objetivo3: Alcanzar un grado de protección deseado contra la pérdida de datos.

Objetivo4: Registrar los eventos relacionados con la seguridad de la información y generar evidencias.

Objetivo5: Garantizar la integridad de los sistemas operacionales para la organización.

Objetivo6: Evitar la explotación de vulnerabilidades técnicas.

Objetivo7: Minimizar el impacto de actividades de auditoría en los sistemas operacionales.

Control	Valoración inicial	Valoración final
[12] Seguridad en las operaciones	33.51%	72.85%
12.1 Procedimientos y responsabilidades operacionales.		
12.1.1 Documentación de procedimientos de operación.	L3	L3
12.1.2 Gestión de cambios.	L2	L3
12.1.3 Gestión de capacidades.	L1	L2
12.1.4 Separación de los recursos de desarrollo, prueba y producción.	L2	L2
12.2 Protección contra código malicioso.		
12.2.1 Controles contra el código malicioso.	L2	L3
12.3 Copias de seguridad.		
12.3.1 Copias de seguridad de la información.	L2	L3
12.4 Registros y supervisión.		
12.4.1 Registro de eventos	L2	L3
12.4.2 Protección de la información de registro.	L2	L3
12.4.3 Registros de administración y operación.	L1	L1
12.4.4 Sincronización de relojes.	L1	L1
12.5 Control del software en explotación.		
12.5.1 Instalación del software en sistemas en producción.	L2	L2
12.6 Gestión de la vulnerabilidad técnica.		
12.6.1 Gestión de las vulnerabilidades técnicas.	L1	L3
12.6.2 Restricciones en la instalación de software.	L0	L2
12.7 Consideraciones de las auditorias de los sistemas de información.		
12.7.1 Controles de auditoria de los sistemas de información.	L0	L3

Tabla 31

[13] Seguridad en las telecomunicaciones

Objetivo1: Evitar el acceso físico no autorizado, los daños e interferencias a la información de la organización y las instalaciones de procesamiento de la información.

Objetivo2: Mantener la seguridad de la información que transfiere una organización internamente o con entidades externas.

Control	Valoración inicial	Valoración final
[13] Seguridad en las telecomunicaciones	2.91%	2.91%
13.1 Gestión de la seguridad de redes.		
13.1.1 Controles de red.	L1	L1
13.1.2 Seguridad de los servicios en red.	L0	L0
13.1.3 Segregación en redes.	L0	L0
13.2 Intercambio de información		
13.2.1 Políticas y procedimientos de intercambio de información.	L0	L0
13.2.2 Acuerdos de intercambio de información.	L0	L0
13.2.3 Mensajería electrónica.	L0	L0
13.2.4 Acuerdos de confidencialidad o no revelación	L1	L1

Tabla 32

[14] Adquisición, desarrollo y mantenimiento de los sistemas de información

Objetivo1: Garantizar que la seguridad de la información sea una parte integral de los sistemas de información en todo el ciclo de vida, incluyendo los requisitos para aquellos que proporcionan servicios en redes públicas.

Objetivo2: Garantizar que la seguridad de la información se diseñe e implemente dentro del ciclo de vida de desarrollo de los sistemas de información.

Objetivo3: Garantizar la protección de los datos que se utilizan para procesos de pruebas.

Control	Valoración inicial	Valoración final
[14] Adquisición, desarrollo y mantenimiento de los sistemas de información	14.07%	21.85%
14.1 Requisitos de seguridad en sistemas de información.		
14.1.1 Análisis de requisitos y especificaciones de seguridad de la información.	L0	L0
14.1.2 Asegurar los servicios de aplicaciones en redes públicas.	L1	L1
14.1.3 Protección de las transacciones de servicios de aplicaciones.	L1	L1
14.2 Seguridad en los procesos de desarrollo y soporte.		
14.2.1 Política de desarrollo seguro de software.	L0	L0
14.2.2 Procedimientos de control de cambios en los sistemas.	L1	L3
14.2.3 Revisión técnica de las aplicaciones tras efectuar cambios en el sistema operativo	L0	L3
14.2.4 Restricciones a los cambios en los paquetes de software.	L2	L3
14.2.5 Uso de principios de ingeniería en protección de sistemas.	L1	L1
14.2.6 Seguridad en entornos de desarrollo.	L2	L2
14.2.7 Externalización del desarrollo de software.	L3	L3
14.2.8 Pruebas de funcionalidad durante el desarrollo de los sistemas.	L1	L1
14.2.9 Pruebas de aceptación.	L1	L1
14.3 Datos de prueba.		
14.3.1 Protección de los datos utilizados en pruebas.	L1	L1

Tabla 33

[15] Relaciones con suministradores

Objetivo1: Garantizar la protección de los activos de la organización que son accesibles a proveedores.

Objetivo2: Mantener el nivel en la prestación de servicios conforme a los acuerdos con el proveedor en materia de seguridad de información.

Control	Valoración inicial	Valoración final
[15] Relaciones con suministradores	5%	5%
15.1 Seguridad de la información en las relaciones con suministradores.		
15.1.1 Política de seguridad de la información para suministradores.	L0	L0
15.1.2 Tratamiento del riesgo dentro de acuerdos de suministradores.	L0	L0
15.1.3 Cadena de suministro en tecnologías de la información y comunicaciones	L0	L0
15.2 Gestión de la prestación del servicio por suministradores.		
15.2.1 Supervisión y revisión de los servicios prestados por terceros.	L1	L1
15.2.2 Gestión de cambios en los servicios prestados por terceros.	L1	L1

Tabla 34

[16] Gestión de incidentes en la seguridad de la información

Objetivo1: garantizar una administración de incidentes de seguridad de la información coherente y eficaz en base a un enfoque de comunicación de los eventos y las debilidades de seguridad.

Control	Valoración inicial	Valoración final
[16] Gestión de incidentes en la seguridad de la información.	5.71%	17.14%
16.1 Gestión de incidentes de seguridad de la información y mejoras.		
16.1.1 Responsabilidades y procedimientos.	L1	L3
16.1.2 Notificación de los eventos de seguridad de la información.	L1	L1
16.1.3 Notificación de puntos débiles de la seguridad.	L0	L0
16.1.4 Valoración de eventos de seguridad de la información y toma de decisiones	L0	L0
16.1.5 Respuesta a los incidentes de seguridad.	L1	L1
16.1.6 Aprendizaje de los incidentes de seguridad de la información.	L1	L1
16.1.7 Recopilación de evidencias.	L0	L0

Tabla 35

[17] Aspectos de seguridad de la información en la gestión de la continuidad de negocio.

Objetivo1: mantener la seguridad de la información integrada en los sistemas de gestión de continuidad del negocio de la organización.

Objetivo2: garantizar la disponibilidad de las instalaciones de procesamiento de información.

Control	Valoración inicial	Valoración final
[17] Aspectos de seguridad de la información en la gestión de la	1.67%	45%

continuidad de negocio		
17.1 Continuidad de la seguridad de la información.		
17.1.1 Planificación de la continuidad de la seguridad de la información.	L1	L3
17.1.2 Implantación de la continuidad de la seguridad de la información.	L0	L3
17.1.3 Verificación, revisión y evaluación de la continuidad de la seguridad de la información	L0	L3
17.2 Redundancias		
17.2.1 Disponibilidad de instalaciones para el procesamiento de la información	L0	L0

Tabla 36

[18] Cumplimiento

Objetivo1: Evitar incumplimientos a requisitos relacionados con la seguridad de la información de cualquier tipo especialmente a las obligaciones legales, estatutarias, normativas o contractuales.

Objetivo2: Garantizar que se implementa y opera la seguridad de la información de acuerdo con las políticas y procedimientos organizacionales.

Control	Valoración inicial	Valoración final
[18] Cumplimiento	17%	48,66%
18.1 Cumplimiento de los requisitos legales y contractuales		
18.1.1 Identificación de la legislación aplicable.	L1	L1
18.1.2 Derechos de propiedad intelectual (DPI).	L2	L2
18.1.3 Protección de los registros de la organización.	L2	L2
18.1.4 Protección de datos y privacidad de la información personal.	L2	L2
18.1.5 Regulación de los controles criptográficos.	L1	L1
18.2 Revisiones de la seguridad de la información.		
18.2.1 Revisión independiente de la seguridad de la información.	L0	L1
18.2.2 Cumplimiento de las políticas y normas de seguridad.	L0	L3
18.2.3 Comprobación del cumplimiento.	L0	L3

Tabla 37

5.5 Resultados

Tras la realización de las valoraciones anteriores, se genera un Informe de Auditoría con los cuadros de resumen de estos. Este informe puede consultarse en el Anexo IX.

En las gráficas generadas, se puede observar una mejora notable en casi todos los aspectos de la seguridad estudiados. Aunque es cierto que falta mucho por hacer, se han mejorado muchos procesos respecto a la gestión de la seguridad de la información, que por si mismos, suponen una mejora para la seguridad de la información de la organización.

6. Conclusiones

Como resumen final, se han obtenido las siguientes conclusiones sobre la ejecución del presente Plan Maestro de Seguridad:

6.1 Situación inicial y objetivos del Plan:

- La organización no disponía de mecanismos ni conocimientos sobre la gestión de la Seguridad de la información, más allá de algunos procedimientos técnicos poco o nada documentados.
- En el pasado, la organización sufrió varios incidentes de seguridad que afectaron a la continuidad del negocio. Sin embargo, no disponía de mecanismos adecuados para evitarlos ni para reducir el impacto causado por estos.
- Debido a estos incidentes, la organización quería conocer el estado de la seguridad de la información en el que se encontraba.
- La organización tenía claro que la normalización y documentación del tratamiento de la información mejora la optimización de recursos y la gestión ante situaciones críticas como los incidentes de seguridad, por lo que, a pesar de no disponer de recursos con formación específica en gestión de la seguridad de la información, estaba interesada en implantar un SGSI. Esta implantación sería el punto de partida para una futura certificación en la norma y también constituiría una mejora de la imagen ante clientes actuales y potenciales, ya que constituye en sí misma una demostración del esfuerzo por la correcta gestión de la seguridad de la información por parte de la organización.

6.2 Objetivos conseguidos

- La Organización es consciente de que debe realizar todas las tareas requeridas en este Plan y mantener la metodología PDCA (PLAN-DO-CHECK-ACT) indicada en él.
- Se han generado los principales documentos base del SGSI, que serán revisados y mejorados en un ciclo continuo.
- Durante el Plan, se realizó un análisis exhaustivo de los activos de la organización, y de sus riesgos y amenazas, lo que permite a la organización disponer de mayor conocimiento para mejorar la protección de los activos y para conocer el impacto de la materialización de esas amenazas.
- Durante la realización de este Plan, la organización ha mejorado considerablemente sus conocimientos sobre la normativa de gestión de la seguridad de la información.
- Muchos de los procedimientos que se utilizaban antes, pero que no estaban escritos o siquiera definidos, han sido identificados y documentados.
- Se han realizado proyectos de mejora que reducirán o evitarán a futuro, los incidentes de seguridad que la organización ha sufrido en el pasado, sobre todo en cuanto a la continuidad de las operaciones y a la explotación de vulnerabilidades en sus sistemas.
- La participación del personal en la ejecución de este plan ha supuesto una mayor concienciación general en la organización respecto a la importancia de la seguridad de la información.

6.3 Objetivos futuros

- Mantener la metodología PDCA, mediante las auditorías internas programadas y la ejecución de proyectos de mejora a partir de las conclusiones de estas.
- Realizar un nuevo Plan Maestro con el objetivo principal de conseguir la certificación en la norma. En este nuevo plan, se buscará la conformidad de todos los controles de la norma menores a L3 y se volverán a generan propuestas de mejora para conseguir estos objetivos.

7. Glosario de términos

Autenticidad: propiedad o característica consistente en que una entidad es quien dice ser o bien que garantiza la fuente de la que proceden los datos. [UNE-71504:2008]

Confidencialidad: Propiedad de la información que se mantiene inaccesible y no se revela a individuos, entidades o procesos no autorizados. [UNE-ISO/IEC 27000:2014]

Integridad: Propiedad o característica consistente en que el activo no ha sido alterado de manera no autorizada. [UNE-71504:2008]

Disponibilidad: Propiedad o característica de los activos consistente en que las entidades o procesos autorizados tienen acceso a los mismos cuando lo requieren. [UNE-71504:2008]

Trazabilidad (imputabilidad): Propiedad o característica consistente en que las actuaciones de una entidad pueden ser imputadas exclusivamente a dicha entidad. [UNE-71504:2008]

8. Bibliografía y referencias

9. Anexos

I. Política de Seguridad
II. Procedimiento de Auditorías Internas
III. Gestión de Indicadores
IV. Procedimiento Revisión por Dirección
V. Gestión de Roles y Responsabilidades
VI. Metodología de Análisis de Riesgos
VII. Declaración de Aplicabilidad
VIII. Proyectos de mejora propuestos
IX. Informe de Auditoría

I. Política de Seguridad

1. Alcance

El alcance de esta política de seguridad será el de todos los empleados de Ingeniería SL, así como los socios, proveedores y clientes que estén relacionados con Ingeniería SL, cuando manipulen, transporten o utilicen información propiedad de Ingeniería SL.

2. Objetivos

Dado que la seguridad de la información es una responsabilidad global y fundamental para Ingeniería SL, todos sus componentes, tienen la obligación de garantizar la Confidencialidad, Integridad y Disponibilidad de la información manejada por Ingeniería SL. Para ello, se establecen una serie de obligaciones y responsabilidades que deberán cumplir todas las partes de Ingeniería SL.

3. Obligaciones del personal de Ingeniería SL

- Notificar al responsable de seguridad de la información, de la forma más rápida posible, cualquier incidencia relacionada con la seguridad de la información o que crean que puede tener impacto sobre esta. Estos incidentes pueden tener diversa naturaleza, siendo algunos ejemplos:

- Pérdida o robo de cualquier almacenamiento de información, como discos externos, documentos, o cualquier otro soporte de información.

- Pérdida o robo de ordenadores, teléfono de empresa u otro hardware propiedad de la Ingeniería SL o que pueda contener información propiedad de Ingeniería SL o de cualquiera de sus socios, proveedores o clientes.

- Borrado accidental de documentos, archivos o bases de datos de la organización.

Se deberá cumplir con una política de “mesas vacías”, de forma que, una vez terminada la jornada laboral, no quede en su puesto de trabajo ningún documento a la vista.

Identificar y clasificar correctamente toda la información generada de acuerdo con las normas de Ingeniería SL.

Notificar al responsable de seguridad de la información, de la salida de cualquier equipamiento de Ingeniería SL o que esté bajo su custodia, para utilizarse fuera de las oficinas de la organización.

Utilizar los recursos de Ingeniería SL, como correo electrónico, ordenadores, conexión a internet, etc., de forma racional y responsable, y siempre con los fines para los que la organización los ha concedido.

Solicitar autorización al responsable de seguridad de la información para la instalación de cualquier software en los equipos de Ingeniería SL.

Asegurarse que la protección antivirus instalada en su equipo funciona correctamente y está al día en cuanto a actualización de firmas.

Mantener la seguridad física de las instalaciones manteniendo siempre cerradas las puertas que dan acceso a la oficina.

Cumplir y asegurar esta política de seguridad.

4. Obligaciones de la organización

Poner a disposición de todos los empleados de un buzón físico o virtual, en cuyo caso debería de ser anónimo, de sugerencias sobre mejoras o consultas sobre la gestión de la seguridad de la información.

Proveer de los recursos hardware necesarios para el transporte y manipulación de información fuera de las oficinas, cuando sea requerido por el trabajo a realizar.

Proveer de usuario y contraseña para el acceso a los diferentes sistemas de Ingeniería SL.

Proveer de una solución antivirus para todos los equipos de la organización.

Mantener un registro de recursos que tengan que estar fuera de la oficina por necesidades de Ingeniería SL, como portátiles, teléfonos móviles o unidades de almacenamiento. Este registro deberá incluir como mínimo, fecha de salida, persona a la que se le asigna, fecha de entrada y firma del responsable de seguridad.

Crear y mantener un plan de recuperación de desastres y proveer de los medios necesarios para su cumplimiento.

Mantener los medios físicos necesarios para garantizar la seguridad física de las instalaciones y su protección razonable respecto a

Comunicar a empleados, socios, proveedores y clientes, esta política de seguridad.

Cumplir y asegurar esta política de seguridad.

5. Responsabilidades

La responsabilidad sobre el cumplimiento de esta política recaerá sobre el responsable de seguridad de la información.

Las posibles sanciones derivadas del incumplimiento de esta política serán propuestas por el responsable de seguridad y autorizadas por director/gerente.

6. Revisión de la política de Seguridad

La política de seguridad deberá ser revisada de forma periódica, en intervalos no mayores a 1 año, o si se producen cambios significativos en la organización de Ingeniería SL. Esta revisión deberá asegurar que la política continúa siendo adecuada y que se está cumpliendo. Asimismo, se deberá evaluar los posibles cambios de esta ante modificaciones o cambios importantes en la organización.

La revisión deberá ser realizada por el responsable de seguridad de la información y deberá ser aprobada por el comité de seguridad de la información.

Una vez revisada y aprobada, la política de seguridad deberá ser comunicada a todo el personal de Ingeniería SL, haya o no sufrido cambios respecto a la versión anterior.

II. Procedimiento de Auditorías Internas

1. Alcance

Este procedimiento cubrirá todas las partes definidas en el alcance de este Plan Maestro de Seguridad, y que fueron descritas al inicio.

2. Responsabilidades de auditoría

Deberá determinarse un equipo de auditoría formado por una o más personas, con los conocimientos necesarios en materia de seguridad de la información o con experiencia en este campo.

El Responsable de Seguridad de la Información de Ingeniería SL, definirá este equipo y será también el Responsable de Auditoría, encargado de garantizar que se lleve a cabo siguiendo los procedimientos y planificaciones establecidos.

El auditor o equipo auditor, deberá ser independiente de los procesos a auditar y deberá de tener conocimientos en materia de seguridad de la información o experiencia en la materia, con el fin de que sus actuaciones estén en línea con la normativa.

Si es posible, se elegirá un auditor externo con independencia total con la organización. Si esto no es posible, se elegirá entre el personal de Ingeniería SL que mejor cumpla los requisitos de independencia con los procesos auditados y formación relacionada. A continuación, se describen estos requisitos:

Formación en Ingeniería o estudios afines.

Experiencia mínima de 2 años relacionada con los sistemas y procesos a auditar.

Conocimientos sobre los principios de auditoría y normativa ISO/IEC 27001.

Capacidad de comunicación.

Actitud positiva

Capacidades de gestión

Independencia de los procesos auditados. Dado que el auditor interno podrá ser un miembro de la organización y esta es pequeña, se asume que no podrá ser totalmente independiente en todos los procesos que audite, por lo que, los procesos donde sea imposible esta independencia serán auditados por otro miembro independiente a estos.

3. Procedimiento de auditoría

Las auditorías aquí definidas, deberán realizarse siguiendo el siguiente procedimiento:

- Reunión inicial: se reunirán el Responsable de Auditoría y el Auditor o equipo auditor, si procede, para determinar los requerimientos y el alcance de la auditoría, la documentación de auditorías previas y los informes de la dirección con los cambios en procesos u organizativos que puedan afectar a los elementos definidos en el alcance.

- Revisión de la documentación: se revisará la documentación existente sobre los procesos a auditar, así como todos los elementos indicados en dicha documentación.

- Revisión in-situ de los elementos auditados: se realizará una revisión de los elementos auditados de acuerdo con las normas ISO/IEC 27001:2013 e ISO/IEC 27002:2013.

- Reunión de finalización: se reunirán el Responsable de Auditoría y el Auditor para verificar que se ha realizado correctamente el proceso de auditoría.

- Realización de informa: el Auditor realizará un informe con los resultados obtenidos (no conformidades) durante el proceso.

4. Planificación de auditorías

Las auditorías internas se realizarán una vez al año, y deberán cubrir al menos un 50% de los dominios definidos en la Declaración de Aplicabilidad del Anexo VII, de forma que cada 2 años se hayan auditado todos los dominios definidos.

5. Informe de auditoría

Al finalizar la auditoría, se realizará un informe por parte del Auditor, que deberá incluir la siguiente información:

Identificación de la organización

Fecha de la auditoría

Responsable de Auditoría

Auditor o equipo auditor

Objetivos y alcance de la auditoría

Conformidad del Sistema de Gestión de la Seguridad de la Información con las normas ISO/IEC 27001:2013 e ISO/IEC 27002:2013

No conformidades detectadas en la auditoría.

A partir de este informe, el comité de seguridad valorará los posibles proyectos para reducir los problemas encontrados. Una vez que hayan sido autorizados los posibles proyectos por

la dirección, el comité de seguridad establecerá las fechas para las siguientes auditorías internas que evaluarán el impacto de los proyectos realizados.

III. Gestión de indicadores

Tabla de indicadores:

Indicador	Auditorías internas realizadas
Descripción	Número de auditorías internas realizadas
Frecuencia	Anual
Valor Objetivo	1
Valor Umbral	0
Responsable	Responsable de seguridad

Indicador	Incidentes de seguridad en equipos
Descripción	Número de incidentes de seguridad detectados en equipos
Frecuencia	Trimestral
Valor Objetivo	0
Valor Umbral	2
Responsable	Responsable de seguridad

Indicador	Incidentes de seguridad en Aplicaciones corporativas
Descripción	Número de incidentes de seguridad (pérdida de datos, accesos no autorizados)
Frecuencia	Trimestral
Valor Objetivo	0
Valor Umbral	0
Responsable	Responsable de seguridad

Indicador	Mantenimiento de equipos
Descripción	Número de mantenimientos preventivos sobre equipos
Frecuencia	Anual
Valor Objetivo	2

Valor Umbral	1
Responsable	Responsable de seguridad

Indicador	Revisiones de software antivirus
Descripción	Número de revisiones del software antivirus instalado
Frecuencia	Trimestral
Valor Objetivo	2
Valor Umbral	1
Responsable	Responsable de seguridad

Indicador	Revisiones de software no autorizado en equipos
Descripción	Número de revisiones de software no autorizado
Frecuencia	Semestral
Valor Objetivo	0
Valor Umbral	3
Responsable	Responsable de seguridad

Indicador	Copias de seguridad realizadas
Descripción	Número de copias de seguridad semanales realizados.
Frecuencia	Trimestral
Valor Objetivo	12
Valor Umbral	11
Responsable	Responsable de seguridad

Indicador	Pruebas restauración backup GIT
Descripción	Número de pruebas de restauración de backup de GIT
Frecuencia	Anual
Valor Objetivo	1

Valor Umbral	1
Responsable	Responsable de seguridad

Indicador	Pruebas restauración backup Redmine
Descripción	Número de pruebas de restauración de backup de Redmine
Frecuencia	Anual
Valor Objetivo	1
Valor Umbral	1
Responsable	Responsable de seguridad

Indicador	Revisión medidas de seguridad físicas
Descripción	Revisión de las medias de seguridad físicas implantadas en la oficina
Frecuencia	Anual
Valor Objetivo	1
Valor Umbral	1
Responsable	Responsable de seguridad.

Indicador	Revisión documentación de procesos
Descripción	Número de documentos de procesos revisados
Frecuencia	Anual
Valor Objetivo	2
Valor Umbral	1
Responsable	Responsable de seguridad

Indicador	Realización documentación de procesos
Descripción	Número de procesos documentados
Frecuencia	Anual
Valor Objetivo	2

Valor Umbral	1
Responsable	Responsable de seguridad

Indicador	Realización documentación de seguridad
Descripción	Número de documentos de seguridad realizados
Frecuencia	Anual
Valor Objetivo	1
Valor Umbral	1
Responsable	Responsable de seguridad

Indicador	Inventario de dispositivos de almacenamiento
Descripción	Inventario de todos los dispositivos que dispongan de almacenamiento de información
Frecuencia	Anual
Valor Objetivo	1
Valor Umbral	1
Responsable	Responsable de seguridad

Indicador	Dispositivos de almacenamiento perdidos/robados
Descripción	Número de dispositivos que dispongan de almacenamiento de información que hayan sido perdidos, robados o extraviados.
Frecuencia	Semestral
Valor Objetivo	0
Valor Umbral	0
Responsable	Responsable de seguridad

IV. Procedimiento de revisión por Dirección

Este procedimiento se realizará una vez al año, y tendrá, al menos la siguiente información de entrada:

- Informes de anteriores revisiones
- Cambios internos o externos que sean relevantes para el SGSI
- Informes de rendimiento del SGSI incluyendo estadísticas sobre:
    - No conformidades y acciones correctivas
    - Mediciones de los indicadores
    - Resultados de auditorias
    - Cumplimiento de los objetivos de seguridad
- Opiniones y propuestas de personal de la organización y clientes.
- Problemas e incidentes reportados.
- Resultados del análisis de riesgos y el estado de las acciones correctivas.
- Oportunidades de mejora

Como salida de la revisión, se realizará un informe, que deberá incluir decisiones sobre las oportunidades de mejora continua y las necesidades de cambios del SGSI, incluyendo, una planificación general de las acciones a tomar.

V. Gestión de roles y responsabilidades

1. Comité de Dirección

Estará formado por:

- Director de Ingeniería SL

- Director de Operaciones

Este comité tendrá las siguientes funciones:

- Hacer de la seguridad de la información un punto de la agenda del Comité de Dirección de Ingeniería SL

- Elegir a los miembros del Comité de Seguridad de la Información y proveerle de los recursos necesarios y establecer sus directrices de trabajo.

- Autorizar la política y las responsabilices generales en seguridad de la información

- Determinar el umbral de riesgo aceptable en seguridad de la información.

- Analizar las consecuencias para la seguridad de la información de los posibles cambios organizativos o funcionales de Ingeniería SL.

- Autorizar el Plan de seguridad de la información y los proyectos e iniciativas en materia de seguridad.

2. Comité de Seguridad de la Información

Estará formado por:

- Director de Operaciones

- Director de TI

Las funciones de este comité serán las siguientes:

- Implantar las directrices del Comité de Dirección

- Asignar roles y funciones en materia de seguridad.

- Presentar al Comité de Dirección, las políticas, normas y responsabilidades de seguridad de la información, para su aprobación.

- Validar el mapa de riesgos y las acciones de mitigación propuestas por el Responsable de Seguridad de la Información.

- Validar el Plan de seguridad de la información o Plan director de seguridad de la información y presentarlo a aprobación al Comité de Dirección. Supervisar y hacer el seguimiento de su implantación.

- Velar por el cumplimiento de la legislación que en materia de seguridad sea de aplicación.

- Promover la concienciación y formación de usuarios y liderar la comunicación necesaria.

- Revisar las incidencias más destacadas.

- Aprobar y revisar periódicamente el cuadro de mando de la seguridad de la información y de la evolución del SGSI.

3. Responsable de Seguridad

En el caso de Ingeniería SL, el Responsable de Seguridad será el director de TI, que, en la estructura actual, se corresponde con el director del área Termosolar.

Funciones:

- Implantar las directrices del Comité de Seguridad de la Información.

- Elaborar, promover y mantener una política de seguridad de la información y proponer anualmente objetivos en materia de seguridad de la información.

- Desarrollar y mantener el documento de Organización de la seguridad de la Información.

- Desarrollar el marco normativo de seguridad y controlar su cumplimiento.

- Actuar como punto focal en materia de seguridad de la información dentro de la compañía, lo cual incluye la coordinación con otras unidades y funciones (seguridad física, prevención, emergencias, relaciones con la prensa...), a fin de gestionar la seguridad de la información de forma global.

- Promover y coordinar entre las áreas de negocio el análisis de riesgos de los procesos más críticos e información más sensible, y proponer acciones de mejora y mitigación del riesgo, de acuerdo con el umbral aceptable definido por el Comité de Dirección.

- Elevar el mapa de riesgos y el Plan de seguridad de la información al Consejo de Seguridad de la Información.

- Controlar la gestión de riesgos de nuevos proyectos y velar por el desarrollo seguro de las aplicaciones.

- Revisar periódicamente el estado de la seguridad en cuestiones organizativas, técnicas o metodológicas. Esta revisión ha de permitir proponer o actualizar el Plan de seguridad de la información, incorporando todas las acciones preventivas, correctivas y de mejora que se hayan ido detectando.
-
- Gestionar el presupuesto asignado y la contratación de recursos cuando sea necesario para la ejecución de las acciones de mejora del SGSI.

- Coordinar acciones con las áreas de negocio para elaborar y gestionar un Plan de continuidad de negocio para Ingeniería SL, basado en el análisis de riesgos y la criticidad de los procesos de negocio, y la determinación del impacto en caso de materialización del riesgo.

- Velar por el cumplimiento de la normativa legal aplicable.

- Definir la arquitectura de seguridad de los sistemas de información, monitorizar la seguridad a nivel tecnológico (gestión de trazas, vulnerabilidades, cambios...), hacer el seguimiento de los incidentes de seguridad y escalarlos al Comité de seguridad de la Información si procede.

- Elaborar y mantener un plan de concienciación y formación en seguridad de la información del personal

- Hacer seguimiento y revisar los incidentes de seguridad, escalándolos al Comité de Seguridad de la Información si procede.

- Coordinar la implantación de herramientas y controles de seguridad de la información y definir el cuadro de mando de la seguridad. Deberá analizar y mantener actualizado dicho cuadro de mando, presentándolo al Comité de Seguridad con la periodicidad que se establezca.

4. Personal en general

Las responsabilidades para cuales empleado de Ingeniería SL serán:

- Mantener la confidencialidad de la información

- Respetar las normas y procedimientos vigentes en materia de seguridad de la información.

- Utilizar adecuadamente las credenciales de acceso a los sistemas

- Respetar la legislación vigente en materia de protección de datos.

- Notificar incidentes de seguridad o situaciones sospechosas de poner peligro la seguridad de la información.

VI. Metodología de Análisis de Riesgos

Para definir esta metodología se tomará como base MAGERIT versión 3. Esta metodología sigue un proceso por fases orientado a la identificación de todos los riesgos de la organización. A continuación, se presentan las fases del modelo:

1. Toma de datos y procesos de información

Definición del alcance del análisis que se va a realizar.

Análisis de procesos de Ingeniería SL y estudio de los riesgos asociados a estos para determinar cuáles de ellos con críticos.

Determinación de la granularidad con la que se realizará el análisis de riesgos y que determinará el nivel de detalle al que se quiera llegar en la toma de datos.

2. Dimensionamiento y establecimiento de parámetros

En esta fase se establecen los parámetros para ejecutar el análisis de riesgos. Estos parámetros serán: valor de los activos, vulnerabilidad, impactos y efectividad del control de seguridad.

Valor de los activos: este parámetro establece una valoración económica a todos los activos de la organización. Para realizar esta valoración, se tendrán que llevar en cuenta los siguientes valores:

- Valor de reposición: es el valor que tiene para la empresa repone el activo en caso de pérdida.

- Valor de configuración: tiempo necesario desde que se adquiere un activo hasta que se configura para poder utilizarse como activo.

- Valor de uso: valor de pérdida para la organización durante el tiempo que no puede utilizar un activo.

- Valor de pérdida de oportunidad: valor potencial por no poder disponer del activo durante un tiempo.

Para la valoración de activos se establecerán varios grupos en función de su valor y se asignará una estimación económica para los activos correspondientes a cada grupo.

De esta forma, tendremos los siguientes grupos:

Valoración	Rango	Valor estimado
Muy alta	20000€ < Valor < 50000	50000 €
Alta	10000€ < Valor < 20000	20000 €
Media	5000 € < Valor < 10000€	10000 €
Baja	1000€ < Valor < 5000€	5000 €
Muy baja	Valor < 1000 €	1000 €

Vulnerabilidad: se define como la frecuencia de ocurrencia de una amenaza, es decir, la frecuencia con que la organización puede llegar a sufrir una amenaza concreta. Podrá calcularse el valor mediante la fórmula:

Vulnerabilidad = frecuencia estimada/ 365 días

A partir de este valor, se puede generar una tabla de vulnerabilidad respecto a la frecuencia con la que pueden suceder:

Vulnerabilidad	Rango	Valor
Frecuencia Muy alta	1 vez al día	365/365 = 1
Frecuencia Alta	1 vez cada 2 semanas	26/365 = 0.071233
Frecuencia Media	1 vez cada 2 meses	6/365 = 0.016438
Frecuencia Baja	1 vez cada seis meses	2/365 = 0.005479
Frecuencia Muy Baja	1 vez al año	1/365 = 0.002739

Impactos: se define el impacto como el porcentaje de pérdida de valor del activo que se pierde en caso de producirse un incidente sobre el activo. A partir de esta definición, se establece también una tabla con los distintos grupos de impacto que se utilizarán para su clasificación:

Impacto	Valor
Muy alto	100%
Alto	75%
Medio	50%
Bajo	20%

Muy Bajo	5%

Efectividad del control de seguridad: este parámetro servirá para valorar como minimizarán los riesgos las medidas de seguridad que se implanten, ya sea reduciendo la vulnerabilidad o el impacto del riesgo, por lo que podemos indicarlo como Valoración de Impacto/Vulnerabilidad. A continuación de genera una tabla de valores para este parámetro:

Valor Efectividad	Valor
Muy alto	95%
Alto	75%
Medio	50%
Bajo	30%
Muy Bajo	10%

3. Análisis de activos

En esta fase se identificarán los activos que posee Ingeniería SL y que son necesarios para su actividad. Aunque solo se llevarán en cuenta los que queden dentro del alcance definido en la primera fase del análisis de riesgos.

Estos activos se clasificarán de la siguiente forma:

Activos físicos: todos los activos hardware utilizados en la organización

Activos lógicos: desarrollos, licencias y elementos de software utilizados por la organización.

Activos de personal: son las personas, desde el punto de vista de los roles que desempeñan en la organización.

Activos de entorno e infraestructura: todos los elementos de infraestructura que requiere la organización para llevar a cabo su actividad, como el cableado, los sistemas de ventilación, etc. En el caso de Ingeniería SL, estos activos se encuentran externalizados y gestionados por la empresa propietaria del edificio donde se encuentran las oficinas.

Activos intangibles: se identificarán así el conocimiento interno, imagen corporativa, credibilidad entre los clientes, y otros elementos intangibles que dan valor a la organización en el mercado.

4. Análisis de amenazas

La amenaza es una situación que puede darse en la organización y que ocasionaría un problema de seguridad en la misma. Estas amenazas se clasifican de la siguiente manera:

Accidentes: se trata de situaciones no provocadas voluntariamente y que no pueden evitarse en la mayor parte de los casos, como pueden ser las interrupciones de servicios que no gestionamos, como un corte en el suministro eléctrico, o desastres naturales o accidentes, como un incendio o inundación.

Errores: son situaciones provocadas involuntariamente por desconocimiento o descuido. Por ejemplo, errores en el uso de los sistemas, en el desarrollo de software, etc.

Amenazas intencionales presenciales: son situaciones provocadas de forma voluntaria y con conocimiento del daño que puede provocar por el propio personal de la organización. Por ejemplo, accesos no autorizados, robo/filtración de información, indisponibilidad de recursos humanos, etc.

Amenazas intencionales remotas: son provocadas por terceras personas ajenas a la organización y de forma voluntaria.

5. Establecimiento de vulnerabilidades

Mediante la metodología MAGERIT no es necesario enumerar las vulnerabilidades, aunque si tenerlas identificadas para estimar su frecuencia sobre un activo.

6. Valoración de impactos

El impacto en un activo es la consecuencia sobre éste de la materialización de una amenaza. Por ello, tendrá que valorarse el daño económico o pérdidas causadas por este.

7. Análisis de riesgos intrínseco

Se trata de los riesgos a los que la organización está expuesta sin tener en cuenta las medidas de seguridad que pueden implantarse. Se puede calcular de la siguiente forma:

Riesgo = Valor del activo x Vulnerabilidad x Impacto

Una vez que se obtengan los valores de riesgo, la organización decidirá el rango aceptable de este. Para ello, se definirán los siguientes rangos de riesgo aceptable:

Nivel aceptable de riesgo	Valor
Alto	75%
Medio	50%
Bajo	25%

8. Influencia de salvaguardas

Las medidas de seguridad de la información o salvaguardas implantadas en la organización tendrán una influencia importante en el impacto causado por una amenaza o en la vulnerabilidad existente, por lo que esta influencia se clasificará como:

- Preventiva: aquella que reducirá la vulnerabilidad

- Correctiva: aquella que reducirá el impacto.

9. Análisis de riesgos efectivos

Una vez aplicadas las salvaguardias correspondientes, se podrá calcular el riesgo efectivo resultante, de la forma:

Valor de riesgo efectivo x Nueva vulnerabilidad x Nuevo impacto =

Valor del activo x (Vulnerabilidad x % de disminución de vulnerabilidad) x (Impacto x % de disminución de Impacto) =

Riesgo intrínseco x % de disminución de Vulnerabilidad x % de disminución de Impacto

10. Evaluación de riesgos

En esta última fase, se deberán de tomar las decisiones para aplicar las medidas de seguridad que se consideren oportunas a partir de la valoración del riesgo aceptable y el coste de aplicar estas medias. Para ello, se buscará reducir todos los riesgos por debajo del umbral que se defina como oportuno. En este punto, la organización deberá decidir si reducir estos riesgos, transferirlos fuera de la organización, o bien aceptarlos.

VII. Declaración de Aplicabilidad.

Controles	Justificación	Aplica
5. POLITICAS DE SEGURIDAD		
5.1 Directrices de la Dirección en seguridad de la información.		
5.1.1 Conjunto de políticas para la seguridad de la información.	Requerido para SGSI	SI
5.1.2 Revisión de las políticas para la seguridad de la información.	Requerido para SGSI	SI
6. ASPECTOS ORGANIZATIVOS DE LA SEGURIDAD DE LA INFORMACION		
6.1 Organización interna.		
6.1.1 Asignación de responsabilidades para la segur. de la información.	Requerido para definición de roles	SI
6.1.2 Segregación de tareas.	Requerido para definición de roles	SI
6.1.3 Contacto con las autoridades.	Requerido para definición de roles	SI
6.1.4 Contacto con grupos de interés especial.	Requerido para definición de roles	SI
6.1.5 Seguridad de la información en la gestión de proyectos.	Requerido para definición de roles	SI
6.2 Dispositivos para movilidad y teletrabajo.		
6.2.1 Política de uso de dispositivos para movilidad.	Requerido para evitar pérdidas y/o robo e información	SI
6.2.2 Teletrabajo.	Requerido para evitar pérdidas y/o robo de información	SI
7. SEGURIDAD LIGADA A LOS RECURSOS HUMANOS		
7.1 Antes de la contratación.		
7.1.1 Investigación de antecedentes.	Requerido para mejorar procesos de selección	SI
7.1.2 Términos y condiciones de contratación.	Requerido para mejorar procesos de selección	SI
7.2 Durante el empleo.		
7.2.1 Responsabilidades de gestión.	Requerido para mejora de procedimientos internos	SI
7.2.2 Concienciación, educación y capacitación en seguridad de la información.	Requerido para mejora de seguridad de la información en general.	SI
7.2.3 Proceso disciplinario.	Requerido para evitar pérdidas y/o robo de información.	SI
7.3 Finalización de empleo o cambio de puesto de trabajo.		
7.3.1 Responsabilidades ante la finalización o cambio	Requerido para evitar pérdidas y/o robo de información.	SI
8. GESTION DE ACTIVOS		
8.1 Responsabilidad sobre los activos.		
8.1.1 Inventario de activos.	Requerido para mejora gestión activos	SI
8.1.2 Propiedad de los activos.	Requerido para establecer responsabilidades ye vitar pérdidas y/o robo de información.	SI
8.1.3 Uso aceptable de los activos.	Requerido para evitar pérdidas y/o robo de información.	SI
8.1.4 Devolución de activos.	Requerido para evitar pérdidas y/o robo de información.	SI
8.2 Clasificación de la información.		
8.2.1 Directrices de clasificación.	Requerido para garantizar la confidencialidad de la información y evitar pérdidas de información.	SI
8.2.2 Etiquetado y manipulado de la información.	Requerido para garantizar la confidencialidad de la información y evitar pérdidas de información.	SI
8.2.3 Manipulado de la información	Requerido para garantizar la confidencialidad de la	SI

	información y evitar pérdidas de información.	
8.3 Manipulación de los soportes		
8.3.1 Gestión de soportes extraíbles.	Requerido para evitar pérdidas y/o robos de información e introducción de malware.	SI
8.3.2 Eliminación de soportes.	Requerido para evitar pérdidas y/o robos de información e introducción de malware.	SI
8.3.3 Soportes físicos en tránsito.	Requerido para evitar pérdidas y/o robos de información e introducción de malware.	SI
9. CONTROL DE ACCESOS		
9.1 Requisitos de negocio para el control de accesos.		
9.1.1 Política de control de accesos.	Requerido para evitar pérdidas y/o robos de información o daños en las instalaciones.	SI
9.1.2 Acceso a las redes y a los servicios de red	Requerido para evitar intentos de explotación de vulnerabilidades y/o robo o destrucción de información.	SI
9.2 Gestión de acceso de usuario.		
9.2.1 Registro y baja de usuario.	Requerido para evitar robo o destrucción de información.	SI
9.2.2 Provisión de acceso de usuario.	Requerido para procesos de entrada de personal.	SI
9.2.3 Gestión de los derechos de acceso con privilegios especiales.	Requerido para reducir errores de administración y evitar robo y/o destrucción de información.	SI
9.2.4 Gestión de información secreta de autenticación de usuarios.	Requerido para evitar suplantación de personalidad y/o robo o destrucción de información.	SI
9.2.5 Revisión de los derechos de acceso de usuario.	Requerido para reducir errores de operación y evitar robo y/o destrucción de información.	SI
9.2.6 Retirada o adaptación de los derechos de acceso	Requerido para reducir errores de operación y evitar robo y/o destrucción de información	SI
9.3 Responsabilidades del usuario.		
9.3.1 Uso de información secreta para la autenticación.	Requerido para evitar suplantación de personalidad y/o robo o destrucción de información.	SI
9.4 Control de acceso a sistemas y aplicaciones.		
9.4.1 Restricción del acceso a la información.	Requerido para evitar robo y/o manipulación indebida de información.	SI
9.4.2 Procedimientos seguros de inicio de sesión.	Requerido para evitar suplantación de personalidad y/o robo o destrucción de información.	SI
9.4.3 Sistema de gestión de contraseñas.	Requerido para evitar suplantación de personalidad y/o robo o destrucción de información.	SI
9.4.4 Uso de utilidades con privilegios de sistemas.	Requerido para reducir errores de administración y evitar robo y/o destrucción de información	SI
9.4.5 Control de acceso al código fuente de los programas.	Requerido para reducir errores de operación y evitar robo y/o destrucción de información	SI
10. CRIPTOGRAFIA		
10.1 Controles criptográficos.		
10.1.1 Política de uso de los controles criptográficos.	Requerido para fomentar y definir el uso de controles criptográficos.	SI
10.1.2 Gestión de claves.	Requerido para gestionar de forma segura las claves criptográficas.	SI
11. SEGURIDAD FISICA Y AMBIENTAL		
11.1 Áreas seguras.		
11.1.1 Perímetro de seguridad física.	Requerido para evitar robo o destrucción de información.	SI
11.1.2 Controles físicos de entrada.	Requerido para evitar robo o destrucción de información.	SI
11.1.3 Seguridad de oficinas, despachos y recursos.	Requerido para evitar robo o destrucción de información.	SI

11.1.4 Protección contra las amenazas externas y ambientales.	Requerido para evitar robo o destrucción de información.	SI
11.1.5 El trabajo en áreas seguras.	Requerido para evitar robo o destrucción de información.	SI
11.1.6 Áreas de acceso público, carga y descarga.	La organización no dispone de áreas de carga y descarga.	NO
11.2 Seguridad de los equipos.		
11.2.1 Emplazamiento y protección de equipos.	Requerido para mejorar seguridad física de los equipos.	SI
11.2.2 Instalaciones de suministro.	Requerido para mantener la continuidad de negocio	SI
11.2.3 Seguridad del cableado.	Requerido para mantener la continuidad de negocio.	SI
11.2.4 Mantenimiento de los equipos.	Requerido para mantener a continuidad y evitar explotación de vulnerabilidades.	SI
11.2.5 Retirada de materiales propiedad de la empresa	Requerido para evitar pérdidas de información.	SI
11.2.6 Seguridad de los equipos y activos fuera de las instalaciones.	Requerido para evitar pérdidas y/o robos de información.	SI
11.2.7 Reutilización o retirada segura de dispositivos de equipos.	Requerido para evitar pérdidas de información.	SI
11.2.8 Equipo de usuario desatendido.	Requerido para evitar pérdidas y/o robos de información.	SI
11.2.9 Política de puesto de trabajo despejado y bloqueo de pantalla.	Requerido para evitar pérdidas y/o robos de información.	SI
12. SEGURIDAD EN LAS OPERACIONES		
12.1 Procedimientos y responsabilidades operacionales.		
12.1.1 Documentación de procedimientos de operación.	Requerido para optimización de procesos de producción y evitar errores de operación.	SI
12.1.2 Gestión de cambios.	Requerido para mejorar la continuidad de negocio y evitar errores de administración.	SI
12.1.3 Gestión de capacidades.	Requerido para mejorar la continuidad de negocio.	SI
12.1.4 Separación de los recursos de desarrollo, prueba y producción.	Requerido para mejorar la respuesta a incidentes y reducir el impacto de ellos.	SI
12.2 Protección contra código malicioso.		
12.2.1 Controles contra el código malicioso.	Requerido para evitar robo o destrucción de información.	SI
12.3 Copias de seguridad.		
12.3.1 Copias de seguridad de la información.	Requerido para la continuidad de negocio.	SI
12.4 Registros y supervisión.		
12.4.1 Registro de eventos	Requerido para análisis de evidencias	SI
12.4.2 Protección de la información de registro.	Requerido para análisis de evidencias	SI
12.4.3 Registros de administración y operación.	Requerido para análisis de evidencias	SI
12.4.4 Sincronización de relojes.	Requerido para análisis de evidencias	SI
12.5 Control del software en explotación.		
12.5.1 Instalación del software en sistemas en producción.	Requerido para evitar errores de administració	SI
12.6 Gestión de la vulnerabilidad técnica.		
12.6.1 Gestión de las vulnerabilidades técnicas.	Requerido para reducir las vulnerabilidades de los sistemas	SI
12.6.2 Restricciones en la instalación de software.	Requerido para evitar la presencia de malware	SI
12.7 Consideraciones de las auditorias de los sistemas de información.		
12.7.1 Controles de auditoria de los sistemas de información.	Requeridos para evitar la presencia de malware y reducir vulnerabilidades.	SI

13. SEGURIDAD EN LAS TELECOMUNICACIONES		
13.1 Gestión de la seguridad de redes.		
13.1.1 Controles de red.	Requerido para evitar pérdidas de información	SI
13.1.2 Seguridad de los servicios en red.	Requerido para evitar pérdidas de información y para la continuidad de la organización.	SI
13.1.3 Segregación en redes.	Requerido para mejorar la respuesta a incidentes y reducir el impacto de ellos.	SI
13.2 Intercambio de información		
13.2.1 Políticas y procedimientos de intercambio de información.	Requerido para evitar pérdidas de información	SI
13.2.2 Acuerdos de intercambio de información.	Requerido para evitar pérdidas de información	SI
13.2.3 Mensajería electrónica.	Requerido para evitar pérdidas de información y para la continuidad de la organización.	SI
13.2.4 Acuerdos de confidencialidad o no revelación	Requerido para evitar pérdidas de información	SI
14. ADQUISICION, DESARROLLO Y MANTENIMIENTO DE LOS SISTEMAS DE INFORMACION		
14.1 Requisitos de seguridad en sistemas de información.		
14.1.1 Análisis de requisitos y especificaciones de seguridad de la información.	Requerido para identificar vulnerabilidades durante la contratación de servicios.	SI
14.1.2 Asegurar los servicios de aplicaciones en redes públicas.	Requerido para evitar robo o perdida de información en aplicaciones en redes públicas.	SI
14.1.3 Protección de las transacciones de servicios de aplicaciones.	Requerido para evitar robo o perdida de información en aplicaciones en redes públicas.	SI
14.2 Seguridad en los procesos de desarrollo y soporte.		
14.2.1 Política de desarrollo seguro de software.	Requerido para garantizar la seguridad de los datos manipulados por el software	SI
14.2.2 Procedimientos de control de cambios en los sistemas.	Requerido para evitar errores de administración y mejorar la continuidad de negocio.	SI
14.2.3 Revisión técnica de las aplicaciones tras efectuar cambios en el sistema operativo	Requerido para la continuidad de negocio	SI
14.2.4 Restricciones a los cambios en los paquetes de software.	Requerido para la continuidad de negocio y evitar instalación de código malicioso. Requerido para procedimientos de actualiación de software.	SI
14.2.5 Uso de principios de ingeniería en protección de sistemas.	Requerido para garantizar la seguridad de los datos manipulados por el software.	SI
14.2.6 Seguridad en entornos de desarrollo.	Requerido para garantizar la seguridad de los datos manipulados por el software desarrollado.	SI
14.2.7 Externalización del desarrollo de software.	Requerido para reducir errores de desarrollo.	SI
14.2.8 Pruebas de funcionalidad durante el desarrollo de los sistemas.	Requerido para evitar errores en la manipulación de la información por el software.	SI
14.2.9 Pruebas de aceptación.	Requerido para procedimientos de actualización de software.	SI
14.3 Datos de prueba.		
14.3.1 Protección de los datos utilizados en pruebas.	Requerido para evitar pérdidas y/o robo de información de clientes.	SI
15. RELACIONES CON SUMINISTRADORES		
15.1 Seguridad de la información en las relaciones con suministradores.		
15.1.1 Política de seguridad de la información para suministradores.	Requerido para gestionar el intercambio seguro de información con proveedores.	SI

15.1.2 Tratamiento del riesgo dentro de acuerdos de suministradores.	Requerido para reducir el impacto de incidentes en los servicios suministrados por terceros.	SI
15.1.3 Cadena de suministro en tecnologías de la información y comunicaciones	Requerido para evitar pérdidas y/o robo de información.	SI
15.2 Gestión de la prestación del servicio por suministradores.		SI
15.2.1 Supervisión y revisión de los servicios prestados por terceros.	Requerido para gestionar la continuidad de negocio.	SI
15.2.2 Gestión de cambios en los servicios prestados por terceros.	Requerido para gestionar la continuidad de negocio.	SI
16. GESTION DE INCIDENTES EN LA SEGURIDAD DE LA INFORMACION		
16.1 Gestión de incidentes de seguridad de la información y mejoras.		
16.1.1 Responsabilidades y procedimientos.	Requerido para optimizar tiempos y respuesta ante incidentes	SI
16.1.2 Notificación de los eventos de seguridad de la información.	Requerido para optimizar tiempos y respuesta ante incidentes	SI
16.1.3 Notificación de puntos débiles de la seguridad.	Requerido para optimizar gestión de incidentes.	SI
16.1.4 Valoración de eventos de seguridad de la información y toma de decisiones.	Requerido para optimizar gestión de incidentes.	SI
16.1.5 Respuesta a los incidentes de seguridad.	Requerido para optimizar tiempos y respuesta ante incidentes	SI
16.1.6 Aprendizaje de los incidentes de seguridad de la información.	Requerido para optimizar gestión de incidentes.	SI
16.1.7 Recopilación de evidencias.	Requerido para mejorar futuras medidas	SI
17. ASPECTOS DE SEGURIDAD DE LA INFORMACION EN LA GESTION DE LA CONTINUIDAD DE NEGOCIO		
17.1 Continuidad de la seguridad de la información.		
17.1.1 Planificación de la continuidad de la seguridad de la información.	Requerido para mejorar la continuidad de la organización.	SI
17.1.2 Implantación de la continuidad de la seguridad de la información.	Requerido para mejorar la continuidad de la organización.	SI
17.1.3 Verificación, revisión y evaluación de la continuidad de la seguridad de la información	Requerido para mejorar la continuidad de la organización.	SI
17.2 Redundancias		
17.2.1 Disponibilidad de instalaciones para el procesamiento de la información	Requerido para mejorar la continuidad de la organización.	SI
18. CUMPLIMIENTO		
18.1 A continuación, se valorarán los controles		
18.1.1 Identificación de la legislación aplicable.	Requerido para cumplimiento legal	SI
18.1.2 Derechos de propiedad intelectual (DPI).	Requerido para cumplimiento legal.	SI
18.1.3 Protección de los registros de la organización.	Requerido para SGSI	SI
18.1.4 Protección de datos y privacidad de la información personal.	Requerido para cumplimiento legal	SI
18.1.5 Regulación de los controles criptográficos.	Requerido para cumplimiento legal	SI

18.2 Revisiones de la seguridad de la información.		
18.2.1 Revisión independiente de la seguridad de la información.	Requerido para SGSI	SI
18.2.2 Cumplimiento de las políticas y normas de seguridad.	Requerido para SGSI	SI
18.2.3 Comprobación del cumplimiento.	Requerido para SGSI	SI

VIII. Propuestas de proyectos

Proyecto 1: Ampliación hardware Estaciones de trabajo		
Plazo	Corto	1 mes
Presupuesto	1 Estación de trabajo completa	6.018,97
	2 Ampliación de 16 GB de memoria RAM	841,88
	2 Discos SSD 500GB	537,2
	Personal interno	(5h) 200
	Total:	7.598,05 €
Responsable	Director área Termosolar (Responsable de Seguridad de la Información)	
Objetivos	Evitar paradas y caídas provocadas por falta de recursos.	
Descripción	Las simulaciones que se realizan habitualmente en las estaciones de trabajo son elementos críticos en la realización de los proyectos y pueden durar muchas horas. Las paradas provocadas por problemas de capacidad del hardware generan pérdidas de tiempos importantes y en muchos casos, toda la simulación, por lo que es necesario reforzar este elemento mediante la adquisición de una nueva estación de trabajo para las simulaciones más exigentes, y la ampliación de 2 de las estaciones existentes con 16GB de RAM cada una y un disco de estado sólido.	
Puntos de control	Disponibilidad de los elementos.	
Mejoras aportadas	Reducción de paradas y retrasos. Redundancia de recursos críticos (mejora en la continuidad de negocio)	
Beneficios colaterales	Mejora de los tiempos de entrega y de imagen ante clientes.	
Riesgos a mitigar	Pérdida de Disponibilidad e Integridad de las estaciones de trabajo.	
Activos relacionados	HW.2 Estaciones de trabajo	
Control	12.1.3 Gestión de capacidades. 17.1 Continuidad de la seguridad de la información. 17.2 Redundancia	

Proyecto 2: Adquisición de SAI			
Plazo	Corto	1 mes	
Presupuesto	1 SAI 5000VA Personal interno Total:		3891 (2h) 80 3971 €
Responsable	Director área Termosolar (Responsable de Seguridad de la Información)		
Objetivos	Evitar pérdidas de datos y de tiempo en reinicios de simulaciones.		
Descripción	La instalación eléctrica de la localización actual, genera frecuentemente pequeños cortes y la infraestructura de alimentación ininterrumpida del edificio no es capaz de mantener ni siquiera varios minutos el servidor o las estaciones de trabajo para guardar los datos correctamente, por lo que es necesario implementar unos medios propios para mantener 3 estaciones de trabajo, el servidor y los dos switches, el tiempo suficiente para el cierre correcto de los sistemas, o bien, mantener en funcionamiento estos, si el corte tiene una corta duración.		
Puntos de control	Disponibilidad del elemento.		
Mejoras aportadas	Eliminar pérdidas de datos provocados por cortes eléctricos. Eliminar retrasos provocados por reinicios en las simulaciones y pruebas ante pequeños cortes eléctricos.		
Beneficios colaterales	Reducción de riesgos de averías en los elementos hardware provocadas por cortes eléctricos y picos de corriente.		
Riesgos a mitigar	Perdida de Confidencialidad, Integridad y Disponibilidad en el servidor y las estaciones de trabajo, así como los datos y procesos que contienen.		
Activos relacionados	HW.1 Servidor HW.2 Estaciones de trabajo HW.10 Switches AUX.3 Sistema de alimentación ininterumpida. D.1 Base de datos REDMINE D.2 Base de datos GIT D.3 Documentación compañía D.4 Documentación interna		

	D.5 Datos clientes D. 6 Datos proveedores D.7 Datos Proyectos
Control	17.1 Continuidad de la seguridad de la información. 17.2 Redundancia

Proyecto 3: Procedimientos de actualización de software			
Plazo	Medio	2 mes	
Presupuesto	Personal interno Total:		(15h) 600 600€
Responsable	Director área Termosolar (Responsable de Seguridad de la Información)		
Objetivos	Establecimiento de procedimientos para la actualización de los sistemas y su seguimiento. Estos procedimientos permitirán el mantenimiento y actualización del software de forma ordenada y homogénea.		
Descripción	Se definirán 2 procedimientos: Procedimiento mensual de revisión y actualización de sistemas operativos y aplicaciones base. Procedimiento mensual de revisión y actualización de aplicaciones críticas GIT y Redmine.		
Puntos de control	Registros mensuales de revisiones y actualizaciones realizadas y pendientes.		
Mejoras aportadas	Reducción de indisponibilidad de los sistemas causados por bugs y por vulnerabilidades conocidas. Reducción de robos de información por ataques que aprovechen vulnerabilidades conocidas.		
Beneficios colaterales	Homogeneización de software		
Riesgos a mitigar	Perdida de Disponibilidad, Confidencialidad e Integridad del software utilizado.		
Activos relacionados	SW.1 Control de versiones GIT SW.2 Gestión de proyectos REDMINE SW.3 SUSE Linux Enterprise SW.4 Ubuntu Linux SW.5 Centos Linux SW.6 MS Windows 10 SW.7 MS Windows 7 SW.8 Libre Office SW.9 Thunderbird SW.10 Antivirus Windows		
Control	12.1.1 Documentación de procedimientos de operación 12.1.2 Gestión de cambios 12.6.1 Gestión de las vulnerabilidades técnicas.		

	12.6.2 Restricciones en la instalación de software. 14.2.2 Procedimientos de control de cambios en los sistemas. 14.2.3 Revisión técnica de las aplicaciones tras efectuar cambios en el sistema operativo 16.1.1 Responsabilidades y procedimientos.

Proyecto 4: Clasificación de registros de proyectos			
Plazo	Medio	6 meses	
Presupuesto	Personal interno Total		(12h) 480 480€
Responsable	Director área Ferrocarril		
Objetivos	Establecimiento de procedimientos para la gestión y almacenamiento de la información generada por los proyectos.		
Descripción	Se definirán procedimientos para identificar, clasificar y almacenar toda la información generada por los proyectos.		
Puntos de control	Revisiones semestrales de proyectos		
Mejoras aportadas	Evitar pérdidas de información. Mejorar el acceso y disponibilidad de la información		
Beneficios colaterales	Mejora de productividad al disponer de procedimientos escritos. Mejora de la curva de aprendizaje para nuevas incorporaciones.		
Riesgos a mitigar	Pérdida de Confidencialidad, Integridad, Disponibilidad y Trazabilidad, en los datos de proyectos y su gestión.		
Activos relacionados	D.7 Datos proyectos		
Control	8.2.1 Directrices de clasificación. 8.2.2 Etiquetado y manipulado de la información. 8.2.3 Manipulado de la información 12.1.1 Documentación de procedimientos de operación. 12.4.1 Registro de eventos 12.4.2 Protección de la información de registro.		

Proyecto 5: Formación interna			
Plazo	Largo	1 año	
Presupuesto	Personal interno:. (3h preparación + 2 h formación) x 6 meses + 2 h asistencia x 2 alumnos x 6 meses Total:		(54h) 2160 2160€
Responsable	Director área Ferrocarril		
Objetivos	Traspaso de información interna sobre nuevos proyectos y nuevas técnicas aplicadas.		
Descripción	Preparación y ejecución de formaciones internas cortas (2-4h) para la transferencia de conocimientos entre especialistas y resto de técnicos implicados en una tecnología.		
Puntos de control	Realización de 1 formación cada 2 meses como mínimo.		
Mejoras aportadas	Reducción de impacto por indisponibilidad del personal.		
Beneficios colaterales	Mejora de la productividad y desarrollo de los técnicos.		
Riesgos a mitigar	Pérdida de disponibilidad de los recursos humanos.		
Activos relacionados	P.2 Director de Área P.3 Ingeniero desarrollo P.4 Ingeniero hardware i+d		
Control	12.1.1 Documentación de procedimientos de operación.		

Proyecto 6: Contrato confidencialidad.			
Plazo	Corto	1 mes	
Presupuesto	Personal interno Total:		(3h) 120 120€
Responsable	Director Ingeniería SL		
Objetivos	Compromiso legal de los empleados internos y externos con la confidencialidad de la información.		
Descripción	Generación de contratos de confidencialidad para garantizar la confidencialidad sobre los datos de la organización.		
Puntos de control	Existencia del documento firmado junto con el contrato del trabajador o representante del servicio externo.		
Mejoras aportadas	Reducción del riesgo de robo de información		
Beneficios colaterales			
Riesgos a mitigar	Perdida de confidencialidad en los recursos humanos		
Activos relacionados	P.1 Director/gerente P.2 Director de Área P.3 Ingeniero desarrollo P.4 Ingeniero hardware i+d P.5 Comercial (externo) P.6 Contabilidad/Facturación (externo) D.1 Base de datos REDMINE D.2 Base de datos GIT D.3 Documentación compañía D.4 Documentación interna D.5 Datos clientes D. 6 Datos proveedores D.7 Datos Proyectos		
Control	7.2.1 Responsabilidades de gestión. 7.2.2 Concienciación, educación y capacitación en seguridad de la información. 7.3.1 Responsabilidades ante la finalización o cambio		

Proyecto 7: Procedimiento de recuperación de desastres.			
Plazo	Corto	1 mes	
Presupuesto	Personal interno Total:		(40h) 1600 1600€
Responsable	Director área Termosolar (Responsable de Seguridad de la Información)		
Objetivos	Reducción del impacto que pueda ocasionar la pérdida total del servidor y la información que contenga.		
Descripción	Realización de procedimiento de recuperación de desastres para el servidor y todo el software y datos alojados en él, de forma que quede completamente documentadas las tareas necesarias para volver a disponer del entorno completo sobre una nueva máquina, en el mínimo tiempo posible, a partir de las copias de seguridad y la documentación generada.		
Puntos de control	Pruebas anuales de recuperación del entorno sobre otra máquina (PC).		
Mejoras aportadas	Mejora de la continuidad de la organización. Reducción de tiempos de recuperación ante caídas de los sistemas o pérdidas de información.		
Beneficios colaterales			
Riesgos a mitigar	Perdida de Disponibilidad e integridad de los datos y aplicaciones críticas..		
Activos relacionados	D.1 Base de datos REDMINE D.2 Base de datos GIT D.3 Documentación compañía D.4 Documentación interna D.5 Datos clientes D. 6 Datos proveedores D.7 Datos Proyectos HW.1 Servidor SW.1 Control de versiones GIT SW.2 Gestión de proyectos REDMINE SW.3 SUSE Linux Enterprise		
Control	17.1.1 Planificación de la continuidad de la seguridad de la información. 17.1.1 Planificación de la continuidad de la seguridad de la información. 17.1.3 Verificación, revisión y evaluación de la		

	continuidad de la seguridad de la información

Proyecto 8: Implantación sistema de gestión de contraseñas		
Plazo	Corto	2 mes
Presupuesto	Personal interno Software KeePass (gratuito) Total:	(40h) 1600 0 1600€
Responsable	Director área Termosolar (Responsable de Seguridad de la Información)	
Objetivos	Homogeneizar, documentar y asegurar la gestión de contraseñas, tanto comunes, como de usuario.	
Descripción	Implantación de software de gestión de contraseñas y procedimientos sobre su utilización y gestión.	
Puntos de control	Pruebas semestrales con muestras de contraseñas guardadas comunes.	
Mejoras aportadas	Seguridad en la gestión de contraseñas	
Beneficios colaterales		
Riesgos a mitigar	Perdida de Disponibilidad de los recursos humanos Pérdida de Integridad, Confidencialidad y Disponibilidad de los datos y aplicaciones.	
Activos relacionados	P.1 Director/gerente P.2 Director de Área P.3 Ingeniero desarrollo P.4 Ingeniero hardware i+d S.1 Servicio de hosting, correo y dominio SW.1 Control de versiones GIT SW.2 Gestión de proyectos REDMINE SW.3 SUSE Linux Enterprise SW.4 Ubuntu Linux SW.5 Centos Linux	

	SW.6 MS Windows 10 SW.7 MS Windows 7 SW.8 Libre Office SW.9 Thunderbird SW.10 Antivirus Windows D.1 Base de datos REDMINE D.2 Base de datos GIT D.3 Documentación compañía D.4 Documentación interna D.5 Datos clientes D. 6 Datos proveedores D.7 Datos Proyectos
Control	9.2.4 Gestión de información secreta de autenticación de usuarios. 9.3.1 Uso de información secreta para la autenticación. 9.4.3 Sistema de gestión de contraseñas.

Proyecto 9: Documentación sobre roles y gestión de permisos de los administradores			
Plazo	Medio	6 mes	
Presupuesto	Personal interno Total:		(30h) 1200 1200€
Responsable	Director área Termosolar (Responsable de Seguridad de la Información)		
Objetivos	Identificar, documentar y procedimentar los roles y permisos requeridos por las aplicaciones, los sistemas operativos y el acceso a los datos.		
Descripción	Se realizará una identificación y documentación de los perfiles requeridos en las aplicaciones, herramientas de administración, y su asignación a los usuarios para todas las aplicaciones críticas. También se realizará un procedimiento de gestión de permisos, donde se definirán los procesos de alta, baja y modificación de permisos para los usuarios, así como las responsabilices de este proceso.		
Puntos de control	Revisión anual de la documentación sobre permisos.		
Mejoras aportadas	Reducción de riesgos por falta de identificación de roles. Reducción de riesgos de errores de administración. Mayor trazabilidad de la información.		
Beneficios colaterales			
Riesgos a mitigar	Perdida de Disponibilidad de los recursos humanos Pérdida de Integridad, Confidencialidad y Disponibilidad de los datos y aplicaciones.		
Activos relacionados	P.1 Director/gerente P.2 Director de Área P.3 Ingeniero desarrollo P.4 Ingeniero hardware i+d SW.1 Control de versiones GIT SW.2 Gestión de proyectos REDMINE SW.3 SUSE Linux Enterprise SW.4 Ubuntu Linux SW.5 Centos Linux SW.6 MS Windows 10 SW.7 MS Windows 7 SW.10 Antivirus Windows		

	D.1 Base de datos REDMINE D.2 Base de datos GIT D.3 Documentación compañía D.4 Documentación interna D.5 Datos clientes D. 6 Datos proveedores D.7 Datos Proyectos
Control	9.2.3 Gestión de los derechos de acceso con privilegios especiales.

Proyecto 10: Procedimiento de contratación y baja			
Plazo	Corto	2 mes	
Presupuesto	Personal interno Total:		(70h) 2800 2800€
Responsable	Director de Ingeniería SL		
Objetivos	Disponer de procedimientos y documentación que garanticen la correcta gestión de la seguridad en lo referente a la contratación y baja de personal.		
Descripción	Procedimiento con todos los pasos necesarios en la contratación de personal y su baja, entre los que se incluirá el método y las acciones necesarias, al menos, que contengan los siguientes procesos: Investigación de antecedentes profesionales de los candidatos. Procesos administrativos requeridos. Entrega y devolución de material y de documentación inicial. Firma de compromiso de confidencialidad Procesos disciplinarios Entrega y confirmación de política de seguridad.		
Puntos de control	Revisión anual del procedimiento		
Mejoras aportadas	Reducción de riesgos asociados a los RRHH.		
Beneficios colaterales			
Riesgos a mitigar	Perdida de Confidencialidad y Disponibilidad en los recursos humanos		
Activos relacionados	P.1 Director/gerente P.2 Director de Área P.3 Ingeniero desarrollo P.4 Ingeniero hardware i+d		
Control	7.1.1 Investigación de antecedentes. 7.1.2 Términos y condiciones de contratación 7.2.1 Responsabilidades de gestión. 7.2.2 Concienciación, educación y capacitación en seguridad de la información. 7.2.3 Proceso disciplinario. 7.3.1 Responsabilidades ante la finalización o cambio		

IX. Informe de Auditoría

1. Introducción

Este Informe de Auditoría se ha realizado tras la ejecución de los proyectos definidos en el Plan Director de Seguridad, como auditoría de cumplimiento de dicho Plan.

2. Identificación de la organización

Ingeniería S.L.

3. Fecha de la auditoría

Auditoría realizada del 22 al 26 de Abril de 2019

4. Responsable de Auditoría

Esta auditoría ha sido realizada bajo la responsabilidad del Responsable de Seguridad de la Información de Ingeniería S.L.

5. Auditor o equipo auditor

Esta autoría ha sido realizada por un auditor externo: Antonio Romero Leña

6. Objetivos y alcance de la auditoría

El objetivo de esta auditoría es, la de valorar si el SGSI implantado cumple con los requisitos definidos en los apartados 4 al 10 de la norma ISO/IEC 27001/2013 y analizar el nivel de madurez de los diferentes controles del Anexo A de la norma.

El alcance corresponderá con el definido en el capítulo 5.3 del Plan Director.

7. Conformidad del Sistema de Gestión de la Seguridad de la Información con las normas ISO/IEC 27001:2013 e ISO/IEC 27002:2013

A continuación, se presentan resumidos los datos de conformidad a partir del análisis realizado:

Requisitos de la norma ISO/IEC 27001:2013	Valoración inicial	Valoración final
4.- Contexto de la organización	5%	90%
5.- Liderazgo	6.7%	90%
6.- Planificación	1,7%	90%
7.- Soporte	5.3%	71,33%
8.- Operación	3.3%	90%
9.- Evaluación del desempeño	0%	90%
10.- Mejora	0%	70%

Tabla 38

Dominios de la norma ISO/IEC 27002:2013	Valoración inicial	Valoración final
[5] Política de seguridad	10%	90%
[6] Aspectos organizativos de la Seguridad de la Información	19.5%	50%
[7] Seguridad ligada a los recursos humanos	5.5%	90%
[8] Gestión de Activos	23.6%	71%
[9] Control de accesos	15.16%	66.67%
[10] Criptografía.	0%	0%
[11] Seguridad física y ambiental	15.17%	57.11%
[12] Seguridad en las operaciones	33.51%	72.8%
[13] Seguridad en las telecomunicaciones	2.91%	2.9%
[14] Adquisición, desarrollo y mantenimiento de los sistemas de información	14.07%	21.8%
[15] Relaciones con suministradores	5%	5%
[16] Gestión de incidentes en la seguridad de la información.	5.71%	17.1%
[17] Aspectos de seguridad de la información en la gestión de la continuidad de negocio	1.67%	45%
[18] Cumplimiento	17%	48.66%

Tabla 39

Sumarizando los diferentes niveles de madurez de todos los controles, se obtiene la siguiente gráfica:

Madurez CMM de los controles ISO/IEC 27002/2013:

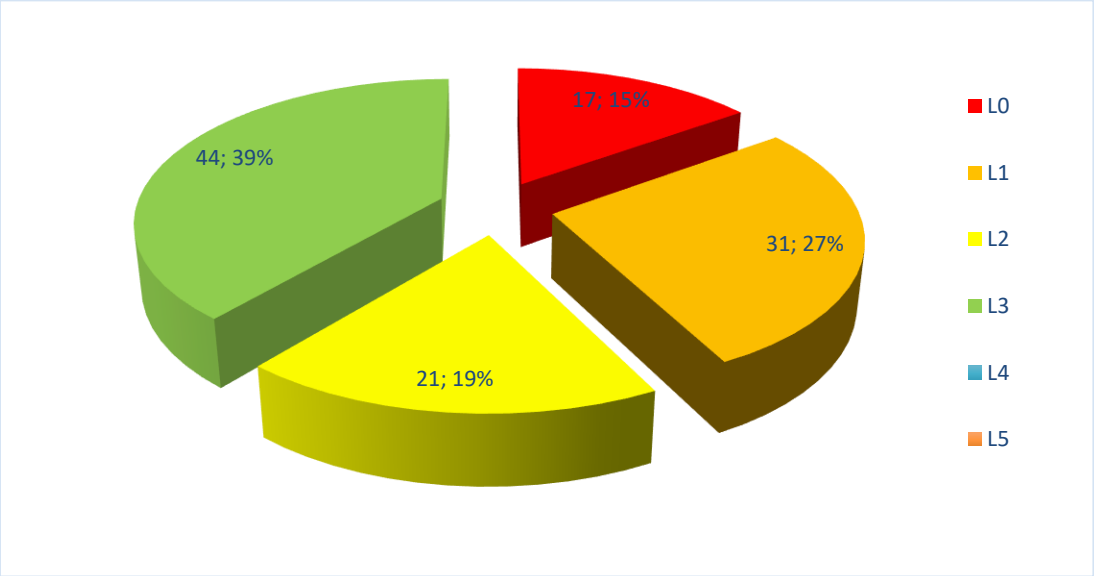


Ilustración 6

De forma más detallada, se puede obtener una gráfica radial con el nivel de cumplimiento de los controles para cada dominio en comparación con el nivel ideal.:

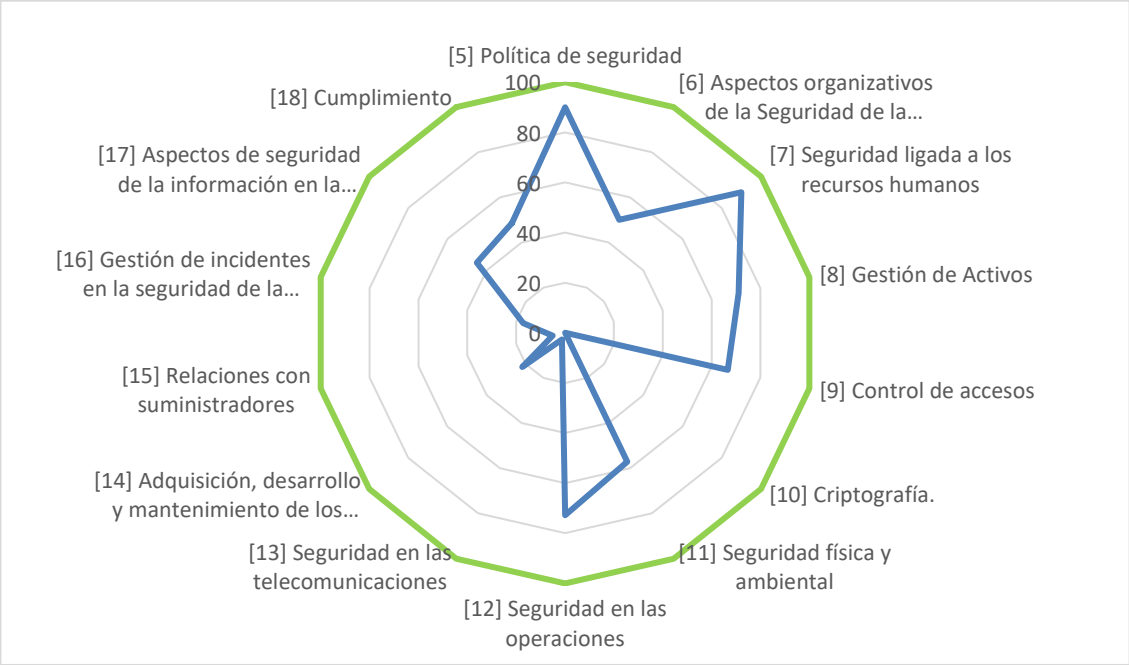


Ilustración 7

8. No conformidades detectadas en la auditoría.

A continuación, se muestran los hallazgos detectados respecto a los requerimientos de la norma ISO/IEC 27001/2013:

Identificador	1
Apartado afectado	7. Soporte (71,33%)
Hallazgo	No conformidad Mayor
Puntos de control afectados	7.2 Competencia 7.4 Comunicación 7.5.2 Creando y actualizando
Descripción	No existe personal interno con la formación suficiente en Seguridad de la información. No están suficientemente definidos los procesos de comunicación internos y externos relativos al SGSI. No están suficientemente definidos los procesos de creación y actualización de toda la documentación. Solo existen para parte de la información.

Acción correctora	Cursos de formación sobre gestión de la seguridad de la información para la dirección. Revisión y creación de documentación de todos los procesos de comunicación interna y externa. Documentación de todos los procesos de creación y actualización de documentación.

Identificador	2
Apartado afectado	10.Mejora (70%)
Hallazgo	No conformidad Mayor
Puntos de control afectados	10.1 No conformidad y acciones correctivas
Descripción	No está suficientemente documentado y claro el tratamiento de los hallazgos encontrados durante las auditorías.
Acción correctora	Revisión y mejora de la documentación del SGSI en cuanto al modelo de autoría.

Aunque hay puntos de control conformes a la normal, otros no conformes, han generado la no conformidad del apartado completo.

Hallazgos detectados respecto a la implementación de los controles descritos en la norma ISO/IEC 27002/2013:

Identificador	3
Dominio afectado	[6] Aspectos organizativos de la Seguridad de la Información (50%)
Hallazgo	No conformidad Mayor
Puntos de control afectados	6.1.2 Segregación de tareas. 6.1.3 Contacto con las autoridades. 6.1.4 Contacto con grupos de interés especial. 6.2.2 Teletrabajo.
Descripción	Las tareas y áreas de responsabilidad no están suficientemente definidas. El contacto con las autoridades existe, pero no está definido y documentado. No existe, salvo necesidades puntuales, contacto definido con grupos u organismos de seguridad especializados. No existe una política definida y documentada sobre el teletrabajo, aunque se realiza cada vez más.

Acción correctora	Hay que revisar y completar la documentación interna y definir las responsabilidades que faltan. Hay que documentar una política de teletrabajo en la que queden definidos los requisitos, métodos de comunicación, etc.

Identificador	4
Dominio afectado	[8] Gestión de Activos (71,11%)
Hallazgo	No conformidad Mayor
Puntos de control afectados	8.1.2 Propiedad de los activos 8.1.3 Uso aceptable de los activos 8.1.4 Devolución de activos 8.3.2 Eliminación de soportes.
Descripción	No está claramente definida la propiedad de los activos. Aunque hay algunas definiciones sobre el uso adecuado de algunos activos, son todavía incompletas. Igualmente, hay que mejorar la política sobre devolución de los activos. Falta por definir la forma de eliminación segura de todos los soportes utilizados.
Acción correctora	Definición y documentación sobre la propiedad de todos los activos del inventario, así como la política, respecto a la devolución de estos. Ampliar y aclarar la definición de uso adecuado de la política. Definir y documentar los métodos seguros requeridos para la eliminación de soportes de información.

Identificador	5
Dominio afectado	[9] Control de accesos (66,67%)
Hallazgo	No conformidad Mayor
Puntos de control afectados	9.2.5 Revisión de los derechos de acceso de usuario. 9.3.1 Uso de información secreta para la autenticación. 9.4.1 Restricción del acceso a la información. 9.4.2 Procedimientos seguros de inicio de sesión. 9.4.4 Uso de utilidades con privilegios de sistemas. 9.4.5 Control de acceso al código fuente de los programas.

Descripción	No están suficientemente definidos los procedimientos de revisión de derechos de acceso a los usuarios. Tampoco está totalmente decididas las responsabilidades del usuario respecto al uso de información de autenticación y el control e acceso a los sistemas y aplicaciones.
Acción correctora	Es necesario ampliar la documentación sobre la gestión de acceso de usuario y sobre todo definir y documentar las responsabilidades del usuario con sus contraseñas y todo lo referente al control de acceso a las aplicaciones.

Identificador	6
Dominio afectado	[10] Criptografía. (0%)
Hallazgo	No conformidad Mayor
Puntos de control afectados	10.1.1 Política de uso de los controles criptográficos. 10.1.2 Gestión de claves.
Descripción	No se dispone de ningún procedimiento ni definición sobre el uso de controles criptográficos, ya que no se hace uso de ellos en general.
Acción correctora	Definir y documentar el uso y la gestión de claves criptográficas.

Identificador	7
Dominio afectado	[11] Seguridad física y ambiental (57.11%)
Hallazgo	No conformidad Mayor
Puntos de control afectados	Están afectados todos los puntos salvo el de política de puesto de trabajo despejado (11.2.9)
Descripción	Se ha mejorado muy poco en este dominio de seguridad, faltando documentar la mayoría de los controles del dominio de Seguridad física y ambiental.
Acción correctora	Definir y crear documentación faltante respecto a las áreas seguras y a la seguridad de los equipos (emplazamiento, protección, cableado, etc.).

Identificador	8
Dominio afectado	[12] Seguridad en las operaciones (72,85%)

Hallazgo	No conformidad Mayor
Puntos de control afectados	12.1.3 Gestión de capacidades. 12.1.4 Separación de los recursos de desarrollo, prueba y producción. 12.4.3 Registros de administración y operación. 12.4.4 Sincronización de relojes 12.5.1 Instalación del software en sistemas en producción. 12.6.2 Restricciones en la instalación de software.
Descripción	Aunque se ha avanzado mucho en este dominio, todavía es necesario mejorar los procedimientos para asegurar la seguridad en las operaciones.
Acción correctora	Crear procedimientos de revisión de equipos y servidores, que incluyan controles de capacidad para los activos críticos y la sincronización de relojes. Definir la segregación correcta de los recursos de desarrollo, prueba y producción. Crear procedimientos para la gestión de registros de administración y operación de los sistemas crítico y de instalaciones y restricciones de software en sistemas en producción.

Identificador	9
Dominio afectado	[13] Seguridad en las telecomunicaciones (2,91%)
Hallazgo	No conformidad Mayor
Puntos de control afectados	No se ha implantado ningún control del dominio de Seguridad en las telecomunicaciones.
Descripción	Prácticamente no existe ningún tipo de gestión sobre la seguridad en las telecomunicaciones.
Acción correctora	Definir y documentar una política sobre seguridad de la red y establecer una división de la red de la organización que permita una mejora gestión de la seguridad. También es necesario ampliar la política de seguridad de la organización, definiendo los procedimientos de intercambio de información con proveedores externos y uso de la mensajería electrónica. Asimismo, será necesario establecer acuerdos de confidencialidad con estos proveedores.

Identificador	10
Dominio afectado	[14] Adquisición, desarrollo y mantenimiento de los sistemas de

	información (21,85%)
Hallazgo	No conformidad Mayor
Puntos de control afectados	14.1 Requisitos de seguridad en sistemas de información. 14.2.1 Política de desarrollo seguro de software. 14.2.5 Uso de principios de ingeniería en protección de sistemas 14.2.6 Seguridad en entornos de desarrollo. 14.2.8 Pruebas de funcionalidad durante el desarrollo de los sistemas 14.2.9 Pruebas de aceptación. 14.3.1 Protección de los datos utilizados en pruebas.
Descripción	Ha mejorado el control sobre este dominio, sobre todo en el área de gestión de cambios, pero siguen faltando muchos controles por establecer correctamente.
Acción correctora	Definir y documentar los controles afectados.

Identificador	11
Dominio afectado	[15] Relaciones con suministradores (5%)
Hallazgo	No conformidad Mayor
Puntos de control afectados	Todos.
Descripción	No existe ningún tipo de política ni gestión definida sobre la relación con proveedores.
Acción correctora	Definir una política de relación con proveedores, donde se tenga en cuenta el tratamiento del riesgo, incluyendo el de la cadena de suministro. También debe incluir la forma de supervisar los servicios prestados por los proveedores y la gestión de cambios de estos servicios.

Identificador	12
Dominio afectado	[16] Gestión de incidentes en la seguridad de la información (17,14%)
Hallazgo	No conformidad Mayor
Puntos de control afectados	Salvo las responsabilidades ante los incidentes, no se han implantado correctamente controles para la gestión de incidentes de seguridad.
Descripción	Aunque la política de la organización ya dispone de algunas indicaciones y normas sobre la gestión de incidentes, es insuficiente para cubrir la gestión de incidentes necesaria para la organización.

Acción correctora	Ampliar la política de seguridad y establecer controles para la correcta gestión de incidentes de seguridad: métodos y normativa de notificación de eventos de seguridad, recopilación de evidencias, su valoración y como se tomarán decisiones ante estos eventos. Hay que establecer también, como se realizará la respuesta a ellos y como se gestionarán las lecciones aprendidas.

Identificador	13
Dominio afectado	[17] Aspectos de seguridad de la información en la gestión de la continuidad de negocio (45%)
Hallazgo	No conformidad Mayor
Puntos de control afectados	17.2.1 Disponibilidad de instalaciones para el procesamiento de la información
Descripción	No se dispone de instalaciones redundadas para una correcta continuidad del negocio en caso de un desastre.
Acción correctora	Estudiar y analizar el uso de la nube para el procesamiento de la información en caso de desastre y ampliar el Plan de continuidad para hacer uso de recursos en la nube si es necesario.

Identificador	14
Dominio afectado	[18] Cumplimiento (17%)
Hallazgo	No conformidad Mayor
Puntos de control afectados	Todos los puntos del dominio de Cumplimiento
Descripción	No se dispone de procedimientos ni otra documentación sobre el cumplimiento de requisitos legales requeridos. Tampoco se ha realizado una revisión independiente de la seguridad de la información.
Acción correctora	

Aunque hay puntos de control conformes a la normal, otros no conformes, han generado la no conformidad en el dominio completo.